



COMPAQ

**Netelligent 2724/2824
Dual-Speed Hubs
User Guide**

©1997 Compaq Computer Corporation. All rights reserved.
Compaq Registered U.S. Patent and Trademark Office.
Company and product names mentioned herein may be
trademarks and/or registered copyright and trademarks of
their respective companies.

.....

NOTICE

The information in this publication is subject to change without notice.

COMPAQ COMPUTER CORPORATION SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL.

This publication contains information protected by copyright. No part of this publication may be photocopied or reproduced in any form without prior written consent from Compaq Computer Corporation.

The software described in this guide is furnished under a license agreement or non-disclosure agreement. The software may be used or copied only in accordance with the terms of the agreement.

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

© 1997 Compaq Computer Corporation.
All rights reserved. Printed in the U.S.A.

Compaq
Registered United States Patent and Trademark Office.

Netelligent is a trademark of Compaq Computer Corporation.

Compaq Netelligent 2724/2824 Dual-Speed Hub User Guide

First Edition (June 1997)
Part Number 299440-001

Federal Communications Commission Notice

Part 15 of the Federal Communications Commission (FCC) Rules and Regulations has established Radio Frequency (RF) emission limits to provide an interference-free radio frequency spectrum. Many electronic devices, including computers, generate RF energy incidental to their intended function and are, therefore, covered by these rules. These rules place computers and related peripheral devices into two classes, A and B, depending upon their intended installation. Class A devices are those that may reasonably be expected to be installed in a business or commercial environment. Class B devices are those that may reasonably be expected to be installed in a residential environment (i.e., personal computers). The FCC requires devices in both classes to bear a label indicating the interference potential of the device as well as additional operating instructions for the user.

The rating label on the device shows which class (A or B) the equipment falls into. Class B devices have an FCC ID on the label. Class A devices do not have an FCC ID on the label. Once the class of the device is determined, refer to the following corresponding statement.

Connections to the serial COM port on this device must be made with shielded cables with metallic RFI/EMI connector hoods in order to maintain compliance with FCC Rules and Regulations.

NOTE: If this equipment contains a Token Ring interface, this equipment is a Class A digital device when the Token Ring interface is utilized.

Class A Equipment

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at personal expense.

Modifications

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Compaq Computer Corporation may void the user's authority to operate the equipment.

Canadian Notice

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Avis Canadien

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

European Union (EU) Notice

Products with the CE Marking comply with both the EMC Directive (89/336/EEC) and the Low Voltage Directive (73/23/EEC) issued by the Commission of the European Community.

Compliance with these directives implies conformity to the following European Norms (in brackets are the equivalent international standards):

- EN55022 (CISPR 22) - Electromagnetic Interference
 - EN50082-1 (IEC801-2, IEC801-3, IEC801-4) - Electromagnetic Immunity
 - UL 1950, Third Edition; CAN/CSA C22.2 No. 950-95, July 1995; TUV Rheinland EN 60950; and 1988 + A1/1990+A2/1991 - Product Safety
-

Japanese Notice

お使いになっている装置にVCCIマークが付いていましたら、次の説明文をお読み下さい。

この装置は、第二種情報装置（住宅地域又はその隣接した地域において使用されるべき情報装置）で住宅地域での電波障害防止を目的とした情報処理装置等電波障害自主規制協議会（VCCI）基準に適合しております。しかし、本装置をラジオ、テレビジョン受信機に近接してご使用になると、受信障害の原因となることがあります。取扱説明書に従って正しい取り扱いをして下さい。

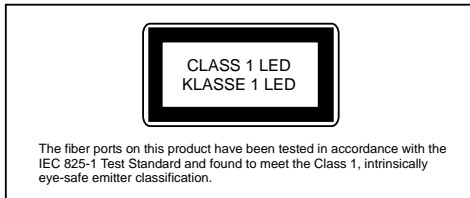
VCCIマークが付いていない場合には、次の点にご注意下さい。

この装置は、商工業地域で使用されるべき第一種情報装置です。住宅地域又はその隣接した地域で使用するとラジオ、テレビジョン受信機等に受信障害を与えることがあります。

Fiber Port Class 1 Classification

Compaq fiber ports have been tested in accordance with the IEC 825-1 test standard and found to meet the Class 1, intrinsically eye-safe emitter classification.

Product Label



Lithium Battery

The non-volatile RAM (NVRAM) chip on the motherboard of the Netelligent 2824 hub contains a non-replaceable lithium battery. Only trained service personnel should dispose of this chip.

La puce mémoire non volatile contient une pile au lithium non remplaçable. L'élimination de cette puce devrait être confiée à un personnel qualifié.



Contents

Chapter 1

Overview

Features	1-2
Package Contents	1-4
Hub Components	1-5
RJ-45 Ports	1-5
Smart Uplink Slot	1-5
LED Indicators	1-6
Serial COM Port	1-8
Host/Target DIP Switch	1-9
Managed/Unmanaged DIP Switch	1-10
Internal 10/100 Switch Disable DIP Switch	1-10
10 ONLY - 10/100 Switch	1-10
10 MDI - 10/100 MDI-X Switch	1-11
Segmentation	1-12

Chapter 2

Planning Installation

Installation Requirements	2-1
Environmental Requirements	2-1
Electrical Requirements	2-1
Spatial Requirements	2-2
Cable Requirements	2-2
System Planning Charts	2-5

Chapter 3

Installing the Hub

Mounting the Hub	3-1
Attaching the Rubber Feet	3-1
Rack-Mounting the Hub	3-1
Installing a Smart Uplink Module	3-3
Inserting the Smart Uplink Module into the Smart Uplink Slot.....	3-3
Connecting Cable.....	3-5
Interconnecting Hubs.....	3-6
Connecting Power.....	3-10
Disconnecting Power.....	3-11
Connecting to the Serial Port.....	3-11

Chapter 4

Configuring the Hub for Management

Setting the IP Address Using VT100.....	4-1
Setting the IP Address Using a BOOTP Server.....	4-7

Chapter 5

Managing the Hub

Management Features	5-1
Management Interface	5-1
SNMP Management.....	5-3
Supported MIBs.....	5-3
Supported Frame Types.....	5-3
IP Frame Types.....	5-4
IP Protocols	5-6
IPX Frame Type	5-7
IPX Protocols.....	5-9
SLIP Protocols.....	5-10

Traps	5-11
RMON Support	5-13
Statistics Group	5-13
History Group	5-14
Alarm Group	5-15
Event Group	5-16
Firmware Updates	5-17
Download Problems	5-18
Parameters Stored in NVRAM	5-19
Compaq Specific Parameters	5-20

Appendix A

Specifications

Physical	A-1
Electrical	A-1
Environmental	A-1

Appendix B

Using the VT100 Interface

Connecting the Hub for VT100	B-1
Setting Up the Communications Program	B-1
Starting the VT100 Interface	B-2
Basic Update Fields	B-4
VT100 Management Options	B-5
Displaying a Data Screen	B-6
Navigating the VT100 Screens	B-6
Viewing System Information	B-8
Viewing the Management Agent Configuration	B-10
Viewing Port Statistics	B-12
Viewing the Stack Configuration	B-13
Viewing and Editing the Backup Port Configuration	B-15

Changing the Password.....	B-17
Downloading Firmware	B-19
Setting Up the Serial Port	B-21
Configuring User Access	B-23
Configuring IP User Access	B-24
Configuring IPX User Access	B-28
Logging Out of the Management Session.....	B-30

Index

Chapter 1

Overview

The Netelligent 2724 and 2824 Dual-Speed hubs feature a 10Base-T and a 100Base-TX repeater in each unit connected by an internal two-port 10/100 Mb/s switch. Each of the hubs' 24 RJ-45 ports automatically detects and adjusts to 10 Mb/s or 100 Mb/s port connection speeds. This makes the hub a perfect solution for networks migrating from 10 Mb/s to 100 Mb/s, allowing you to move from 10 Mb/s to 100 Mb/s speeds on a port-by-port basis. The 100 Mb/s repeater is a 100Base-TX Class I repeater.

The 2824 hub is a *managing* hub, which means it contains a built-in management agent.

The 2724 hub is a *manageable* hub, which means it does not contain a management agent but can be managed by a hub that does contain a management agent (2624 or 2824 hub, provided they are running v2.0 or higher management firmware). To be managed by a managing hub, the 2724 must be connected to a managing hub's connectors on its back panel. Up to five hubs (one managing 2824 or 2624 and four manageable 2524 or 2724) can exist in a single stack for a total of up to 125 ports (with SUMs installed).

Features

The 2724/2824 hub provides the following set of features:

24 RJ-45 ports — allows 10 Mb/s or 100 Mb/s connections by autodetecting the wire speed.

Stackable — lets you stack up to five hubs (four manageable 2724 hubs and one managing 2824 hub) for up to 125 workstation connections. You can also interconnect the 2724/2824 hubs with Netelligent 2524/2624 hubs.

Host/Target Design — allows manageable hubs (Model 2724) to be managed by a single managing hub (Model 2824)

24 Bi-Colored LED Indicators — show port activity, port link, and port disable/auto partition; other LEDs show collisions, the power supply status, and the management status of the hub and the mode (10 or 100).

Backup Ports — provide redundant port connections for mission-critical applications (for example, order entry PCs connected to a file server).

Intrusion Detection — provides a method of preventing unauthorized stations from transmitting on the network.

Field-Upgradable Firmware — lets you upgrade the 2824 hub firmware using XMODEM and TFTP downloads via the BOOTP/TFTP sequence, the VT100 interface, or through SNMP. VT100 and SNMP can occur through both in-band and out-of-band (SLIP) connections.

4-group RMON (Groups 1, 2, 3 & 9) — allows remote monitoring and gathering of network statistics without generating network traffic.

Compaq Netelligent Management Software — provides an easy-to-use graphical interface for managing the hub.

SNMP management over IP and IPX — lets you monitor and manage the hub via any industry-standard SNMP application, such as Compaq Netelligent Management Software (provided at no extra charge with each unit).

VT100 interface — allows out-of-band (serial port) and in-band (Telnet) management for setting numerous configuration parameters.

Rack Mount Kit — lets you install the hub in a standard EIA 19-inch equipment rack.

10/100 Switch Enable/Disable — lets you enable or disable the internal 10/100 switch if the network uses an external bridge or router.

Multicast/Broadcast Filtering — allows the hub to forward or block multicast and broadcast packets independently on both the 10 and 100 Mb/s segments.

Statistics — Separate statistics, similar to those available on the 10 and 100 Mb/s repeater ports, are available for both the 10 and 100 Mb/s ports on the 2-port 10/100 switch.

Smart Uplink Module Support — allows the 2724/2824 hub to uplink to another 2724/2824 hub to overcome the single repeater hop restriction for Class I 100Base-T repeaters.

IP/IPX Autodiscovery — allows the hub to be autodiscovered by network management platforms such as Novell ManageWise, HP OpenView, SunNet Manager, IBM NetView 6000.

Fast Ethernet Wiring Standards — ensures compatibility with all types of UTP cabling.

Three-Year Limited Warranty

Package Contents

Before you start to install the hub, verify that this package contains the following items:

- Netelligent 2724 or 2824 Dual-Speed Hub
- AC power cord
- Rack-mounting kit (two mounting brackets, eight 3/8-inch bracket screws, and four 1/2-inch rack-mount screws)
- Four adhesive-backed rubber feet
- Compaq Netelligent Management Software
- *Compaq Netelligent 2724/2824 Dual-Speed Hub Quick Install Guide*
- *Compaq Netelligent 2724/2824 Dual-Speed Hub User Guide CD*
- Safety compliance guide
- Registration card

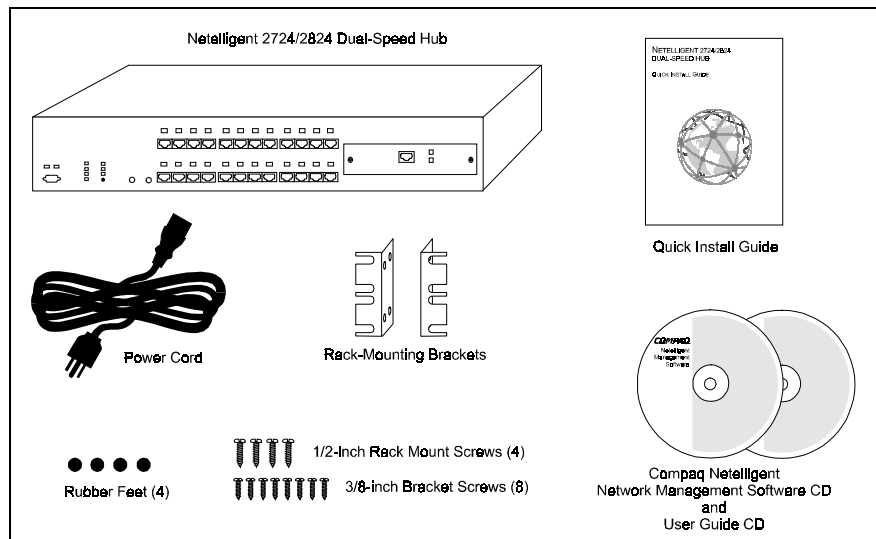


Figure 1-1. Package Contents

Hub Components

This section provides an overview of the hub's components including the LED indicators, RJ-45 ports, and fiber ports. Figure 1-2 shows the hub's front panel.

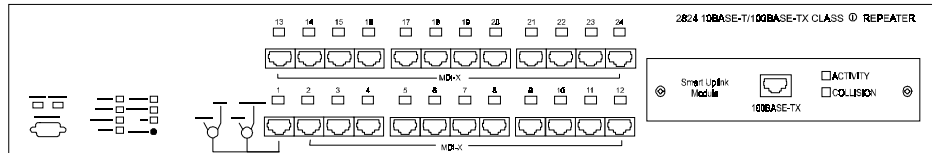


Figure 1- 2. 2724/2824 Hub Front Panel with Smart Uplink Module Installed

RJ-45 Ports

The hub's RJ-45 ports allow connections to UTP cabling to workstations and servers in a 10Base-T or 100Base-TX network. The hub automatically detects the wire speed and adjusts accordingly. You can force Port 1 to run at 10 Mb/s by setting the 10 Mb/s ONLY / 10/100 switch on the front panel to 10 ONLY. You can also use Port 1 as an uplink port by setting the MDI / MDI-X switch to the MDI position. See "MDI / MDI-X Switch" and "10 Mb/s ONLY / 10/100 Switch" for more information.

Smart Uplink Slot

The Smart Uplink slot houses an optional Smart Uplink Module (SUM), which serves as a connection point between hubs, hub stacks, and other manufacturers' 100Base-TX, 100Base-TX(SC), 100Base-TX(ST) hubs or stacks. Smart Uplink modules let you extend your network without the usual repeater hop limitations inherent with Class I repeaters.

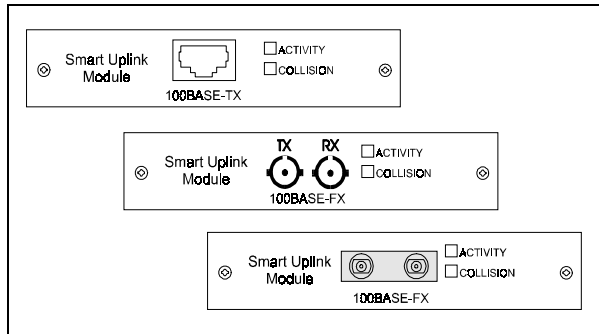


Figure 1- 3. Smart Uplink Modules

The SUM provides two status LEDs: activity and collision. The activity LED is a solid green when the link is active and flashes green when there is activity on the port. The collision LED flashes yellow when a collision is detected and lights solid yellow when the port is disabled. The collision LED does not reflect conditions at the SUM's hub port, only at the external interface port.

LED Indicators

The LED panel of the 2724/2824 hub helps you monitor the hub's operation. When you power on a hub, it performs a power-on self test (POST) which lasts about 1 minute. After the POST, all LEDs reflect the current operational modes which are described in Table 1-1.

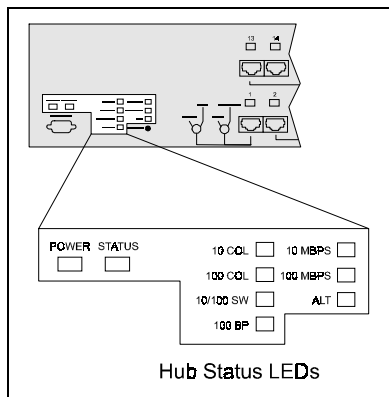


Figure 1- 4. Hub Status LEDs

Table 1-1
2724/2824 LEDs

LED	Status and Description
POWER	<p>Green — The power supply is operating properly. Off — The hub is not powered on.</p>
STATUS	<p>2824 Managing Hub:</p> <p>Off — A basic failure occurred where the firmware agent cannot execute code or the LED control cannot be accessed Yellow — The firmware agent is in the process of booting up and is not ready for management processing. Flashing Yellow — The firmware encountered a failure during the POST. The LED is yellow for one second and off for one second. Flashing Yellow/Green — The hub is operational, but the agent detected a hardware error such as an NVRAM failure or internal 2-port 10/100 switch failure. The LED is yellow for one second and green for one second. Green — The firmware agent has finished booting and is now ready for any management processing.</p> <p>2724 Manageable Hub (in a managed stack):</p> <p>Off — The hub is not being managed by the stack's managing hub. This indicates either a Host/Target switch misconfiguration or a hardware problem. The STATUS indicator is always off if the 2724 hub is in an unmanaged stack. Flashing Green — The hub has its MAN/UNM switch set to UNM (unmanaged). The LED is green for one second and off for one second. Flashing Yellow/Green — The hub is operational, but the agent detected a hardware error such as an internal 2-port 10/100 switch failure. The LED is yellow for one second and green for one second. Green — The hub is properly configured and is being managed by the stack's managing hub.</p>
10 COL (Collision)	<p>Flashing Yellow — Collisions on the 10 Mb/s segment OFF — No collisions on the segment</p>
100 COL (Collision)	<p>Flashing Yellow — Collisions on the 100 Mb/s segment OFF — No collisions on the segment</p>

continued

LED	Status and Description
10/100 SW (Switch)	Flashing Yellow — Internal 10/100 switch problems, such as buffer overflows, address table full Green — Internal 10/100 switch is enabled OFF — Internal 10/100 switch is disabled; 10 Mb/s segment is isolated
100 BP (Backplane)	Green — 100 Mb/s connected to a 100 Mb/s backplane OFF — 100 Mb/s isolated from the 100 Mb/s backplane
ALT (Alternating)	Green — Port LEDs alternate between 10 Mb/s and 100 Mb/s status OFF — Alternating mode off
Mode button	Disables the alternating mode and selects 10/100 port LED display
100 MBPS (Management Port)	Green — Port LEDs show 10 Mb/s status OFF — Port LEDs do not show 10 Mb/s status
10 MBPS (Management Port)	Green — Port LEDs show 100 Mb/s status OFF — Port LEDs do not show 100 Mb/s status
Smart Uplink Module (SUM-TX)	
Activity	Flashing Green — 100 Mb/s traffic occurring on the module Green — Link active, no traffic on the module OFF — No link
Collision	Flashing Yellow — Collisions on the module OFF — No collisions

Serial COM Port

The 2824 (managing) hub contains a serial COM port that uses a DB9 connector with a standard AT pinout. This port lets you perform the following operations:

- XMODEM firmware downloads
- VT100 console interface for basic management and initially setting the IP address
- SLIP (Serial Line Internet Protocol) transfers, including remote (out-of-band) management, SNMP, Telnet, and TFTP firmware downloads.

See Chapter 4 “Configuring the Hub for Management” and Appendix B “Using the VT100 Interface” for more information about the serial port.

Host/Target DIP Switch

On the back panel of the 2724 hub is a HOST/TARGET DIP switch that determines whether the hub is a *host* or *target* hub in a hub stack. For example, you can connect up to two 2724 hubs and designate one as the host and the other hub as a target for an unmanaged stack. Or, if you have a managing hub (2824) in the stack, you can set up to four 2724 manageable hubs as target hubs for a managed stack. The 2824 hub does not have a HOST/TARGET DIP switch.

NOTE: There may be only one host hub in a stack. More than one host hub prevents the stack from passing Ethernet traffic or management commands between units.

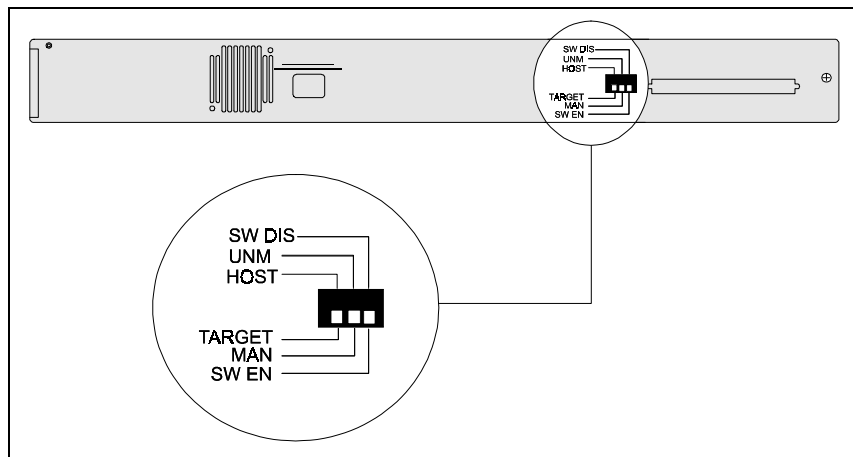


Figure 1- 5. 2724 Hub DIP Switches

Managed/Unmanaged DIP Switch

On the back panel of the 2724 hub is a MAN/UNM DIP switch that sets the hub's initial 100 Mb/s port enable/disable and backplane connection status. When the switch is set to "MAN," the hub sets the initial 100 Mb/s port enable/disable and backplane connection status. When the switch is set to "UNM," the initial 100 Mb/s port and backplane status is set to the hardware default (enabled). The 2824 hub does not have a MAN/UNM DIP switch.

NOTE: When a managing hub is present, it can set port statuses regardless of the switch setting.

Internal 10/100 Switch Disable DIP Switch

The internal 10/100 switch disable DIP switch, located on the back panel of the 2724 hub, lets you disable the internal two-port switch. When you set the switch to "SW DIS," the internal switch is disabled, preventing 10 Mb/s packets from being forwarded to the 100 Mb/s segment and vice-versa. This effectively isolates the 10 Mb/s segment and disables connectivity to the management agent. When you set the switch to "SW EN," the internal switch allows packets to be forwarded between the 10 Mb/s and 100 Mb/s segments, unless the switch is disabled by the management agent.

If you set the DIP switch to "SW EN," you can enable and disable the switch using the *n2feTen100SwEnable* MIB variable. However, if you set the DIP switch to "SW DIS," the hardware disables the bridge, which the management agent cannot change.

You can view the status of the internal switch in the Netelligent 2000/FE (Fast Ethernet) MIB variable *n2feTen100SwHardwareDisableSwitchStatus*.

10 ONLY - 10/100 Switch

The 10 ONLY - 10/100 switch, located on the front panel of both 2724 and 2824 hubs, lets you set the allowable connection types for Port 1. When you set the switch to "10 ONLY," Port 1 allows 10 Mb/s connections only. When you set the switch to "10/100," Port 1 allows 10 Mb/s or 100 Mb/s connections.

If the switch is set to “10/100,” you can force 10 Mb/s connections using the *n2fePortAutoNegCapAdvertised* MIB variable. However, if the switch is set to “10 ONLY,” the hardware forces the connection speed and cannot be changed by the management agent. To view the status of this switch, see the *n2feForce10 Mb/sSwitchStatus* MIB variable.

NOTE: This switch must be set to 10 ONLY if you set the 10 MDI / 10/100 MDI-X switch to 10 MDI.

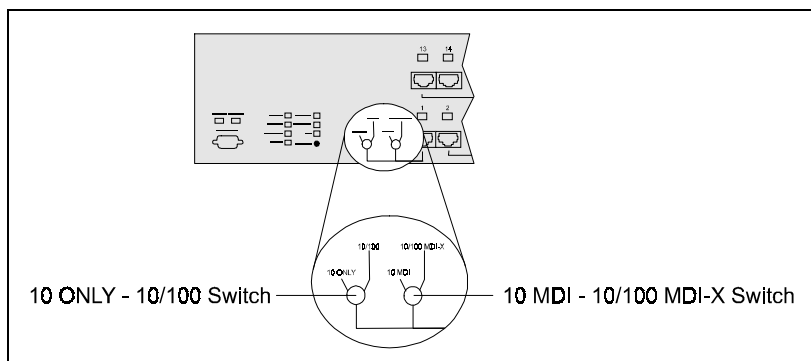


Figure 1- 6. Port 1 Switches

10 MDI - 10/100 MDI-X Switch

The 10 MDI / 10/100 MDI-X switch is located on the front panel of the 2724 and 2824 hubs. This switch lets you set Port 1 as an MDI 10Base-T (uplink) port (for connecting to another hub) or as an MDI-X port (for connecting directly to a network controller card). The 10 MDI setting is for 10Base-T connections only.

NOTE: If you set this switch to 10 MDI, be sure the 10 ONLY - 10/100 switch is set to 10 ONLY.

Segmentation

A *segment* is a single collision domain where all network traffic within that domain contends for the same bandwidth. The Netelligent 2724/2824 hub has a 10 Mb/s segment and a 100 Mb/s segment that are connected via an internal two-port (10 Mb/s / 100 Mb/s) switch. The process of *segmentation* lets you isolate the 10 Mb/s segment from the 100 Mb/s segment, which prevents packet forwarding between the two segments and isolates the hub's 10 Mb/s segment from the common 100 Mb/s backplane. This can improve the bandwidth in your network by reducing the number of nodes that contend for the same segment thereby reducing collisions. For information about isolating the 10 Mb/s segments, see "Internal 10/100 Switch Disable DIP Switch."

You can also isolate the hub's 100 Mb/s segment from the common 100 Mb/s backplane in a stack. To do so, view the Stack Configuration screen of the VT100 interface and set the Backplane Status field to "Isolated" (see "Appendix B – Using the VT100 Interface" for more information). Or, set the *n2feBkplnStatus* MIB variable using a MIB browser or SNMP management application such as Compaq Netelligent Management Software.

All 2824/2724 ports have access to the management agent regardless of connection speed as long as they have access to the stack's common 100 Mb/s backplane. When any hub's internal 10/100 switch is disabled, its 10 Mb/s connections lose their access to the agent. When a manageable hub (2724) is isolated from the common 100 Mb/s backplane, all ports lose their access to the management agent. 100 Mb/s connections on the managing (2824) hub always have access to the agent, regardless of the hub's configuration.

Chapter 2

Planning Installation

This chapter contains installation requirements and system planning charts that will help you prepare for installing the hub.

Installation Requirements

To help ensure a correct installation, read this section to determine the environmental, electrical, spatial, and cable requirements.

Environmental Requirements

Be sure the operating environment for the hub is within the following ranges:

- Temperature: 32° to 104° F (0° to 40° C)
- Humidity: 5% to 95% (non-condensing)
- Altitude: 0 to 10,000 feet (0 to 3 km)
- Clearance: minimum of 2 inches (5.1 centimeters) on each side of the hub (for proper ventilation)

Electrical Requirements

The electrical requirements for the hub are as follows:

- Voltage: 100 to 240 VAC
- Power: 2.0A (@ 100 VAC) to 1.0A (@ 240 VAC)
- Frequency: 50 to 60 Hz



CAUTION: The power outlet must be a non-switched, three-pronged, grounded outlet. Do not use a three-to-two pronged adapter at the outlet. Doing so may result in electrical shock and/or damage to the hub and will void your warranty.

Spatial Requirements

The hub dimensions are 2.5 x 17 x 13.5 inches, 6.4 x 43.6 x 34.6 cm (HxWxD).

Be sure to allow at least 2 inches (5.1 centimeters) on each side of the hub for proper air circulation and cable connections.

Cable Requirements

The following information states the required cable type and distance limitations for 10Base-T, 100Base-TX, and 100Base-FX.

10Base-T

The 10Base-T twisted-pair wiring you connect to the hub's RJ-45 ports must meet the following minimum specifications and requirements to ensure long-term LAN reliability.

- The wiring must be unshielded twisted-pair (UTP), Category 3 or better.
- Two pairs of wiring are required.
- The building codes may require different insulation materials.
- The wire gauge should be between 18 and 26 AWG. (Most telephone installations use 24-gauge wiring.)
- UTP wire should meet the following requirements:
 - Solid copper
 - Nominal capacitance: less than 16 pF/ft
 - Nominal impedance: 100 Ohms
 - Nominal attenuation: less than 11.5 db

100Base-TX

100Base-TX is the IEEE 802.3u specification for transmitting 100 Mb/s Fast Ethernet over two pairs of copper wire. The pinout, connectors (RJ-45 modular plugs), and protocol (CSMA/CD) are exactly the same as for 10Base-T.

Unshielded Twisted Pair (UTP)

- Category 5 only
- Two pairs used (same as 10Base-T)
- Maximum 100-meter (328-foot) link

Figure 2-1 shows a one-to-one cable pinout for 100Base-TX.

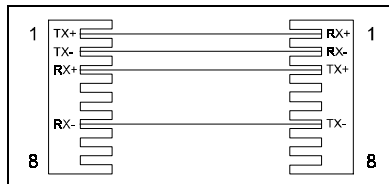


Figure 2- 1. One-to-One Cable Pinout for 100Base-TX

NOTE: To prevent potential electromagnetic interference, terminate the unused wires (4, 5, 7, and 8).

Tables 2-1 and 2-2 show the wiring for straight-through and crossover twisted-pair cable.

Table 2- 1
Straight-Through Twisted-Pair Wiring

Twisted Pair Number	Pin Number	Signal Description	To	Pin Number	Signal Description
1	1	TD+	→	1	TD+
	2	TD-	→	2	TD-
2	3	RD+	→	3	RD+
	6	RD-	→	6	RD-

Table 2-2
Crossover Twisted-Pair Wiring

Twisted Pair Number	Pin Number	Signal Description	To	Pin Number	Signal Description
1	1	TD+	➔	3	RD+
	2	TD-	➔	6	RD-
2	3	RD+	➔	1	TD+
	6	RD-	➔	2	TD-

100Base-FX

100Base-FX is the IEEE 802.3u specification for transmitting 100 Mb/s Fast Ethernet over two strands (one pair) of fiber optic cable. The 2724/2824 hub supports both SC type (low-cost fiber optic interface connector) and ST (optical medium connector plug and socket) connections.

Cable Type

- Fiber optic
- Multi-mode 62.5/125 to 100/150 micron fiber
- Both strands used

System Planning Charts

The charts in Figures 2-2 and 2-3 provide a convenient way of planning the connections for your hub.

2724/2824 Hub Setup and Cabling Chart

Date

Unit Number

Building

Location

Rack Mount

Table Mount

MAC Address

IP Address

Installed Uplink Module

- None
- TX
- FX (ST Type)
- FX (SC Type)

Port	Connects To
24	
23	
22	
21	
20	
19	
18	
17	
16	
15	
14	
13	
12	
11	
10	
9	
8	
7	
6	
5	
4	
3	
2	
1	
Uplink Module	

Figure 2- 2. Hub Setup and Cabling Chart

Rack Inventory Chart

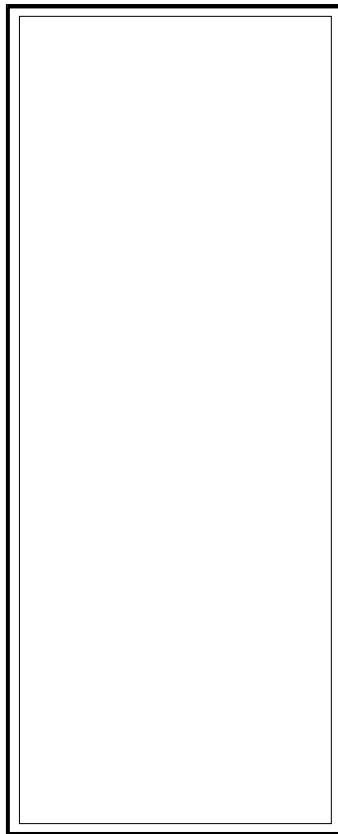
Date

Use this chart to record the devices installed in a particular rack.

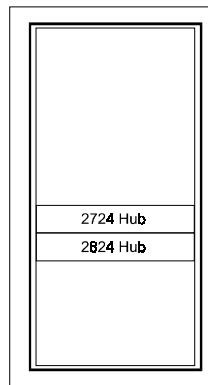
Wiring Closet Number

Rack Number

Installer



Example



2724 Hub
2824 Hub

Figure 2- 3. Rack Inventory Chart

Chapter 3

Installing the Hub

This chapter explains how to mount the hub, attach cables, and connect power.

Mounting the Hub

You can place the hub on a level surface (table top or shelf, for example) or mount it in a standard EIA 19-inch rack.

Attaching the Rubber Feet

If you will place the hub on a table top or shelf, attach the supplied adhesive-backed rubber feet, as described in the following steps.

1. Turn the hub over so that its bottom side faces up.
2. Remove the four rubber feet from their packaging.
3. Peel the protective paper backing off the rubber feet. Then position the feet in the recessed areas near the corners of the hub and press the feet into place.
4. Turn the hub to its upright position and place it on the mounting surface.

NOTE: Be sure you allow at least 2 inches (5 cm) on each side of the hub for proper air flow.

Rack-Mounting the Hub

The hub occupies 1 ½ slots in a standard 19-inch rack. To mount the hub in a rack, use the supplied installation kit. This kit includes two side mounting brackets, eight bracket screws, and four larger rack-mount screws.

3-2 Installing the Hub

To attach the brackets, follow these steps:

1. Remove the two screws from the left and right side of the hub. (These screws are extras and are not needed to install the mounting brackets.)
2. Position the bracket as shown in Figure 3-1 and secure it with the smaller bracket screws. Then attach the remaining bracket to the other side of the hub.

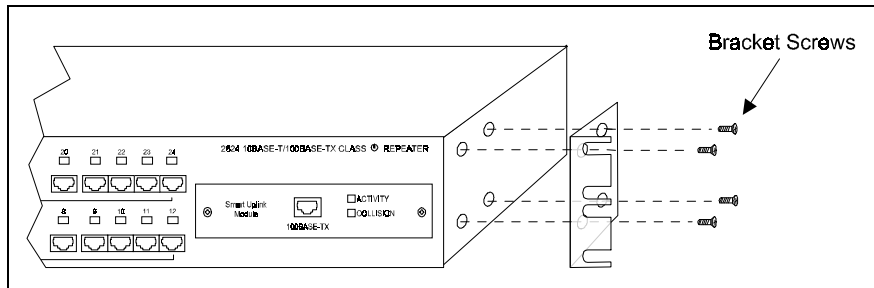


Figure 3- 1. Attaching the Mounting Brackets

3. After you attach both mounting brackets, position the bracket slots over the desired holes on the rack (Figure 3-2). Then insert and tighten the supplied rack-mount screws.

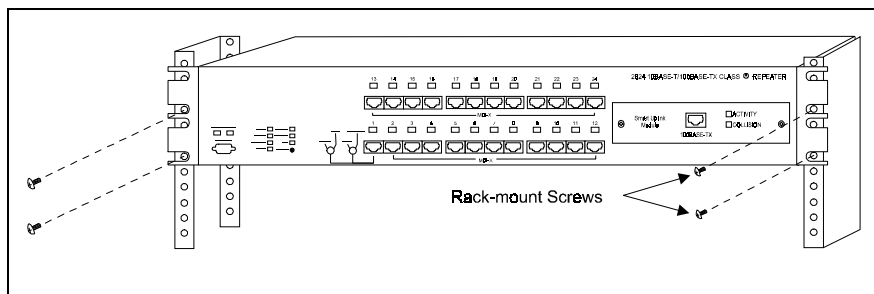


Figure 3- 2. Positioning the Hub in a Rack

Installing a Smart Uplink Module

The Netelligent 2724/2824 hubs have a Smart Uplink slot that lets you install one of the following optional Smart Uplink modules (SUMs):

- ① 100Base-TX version (Part No. 267045-001)
- ② 100Base-FX (fiber) version with ST connector (Part No. 267042-001)
- ③ 100Base-FX (fiber) version SC connector (Part No. 267043-001)

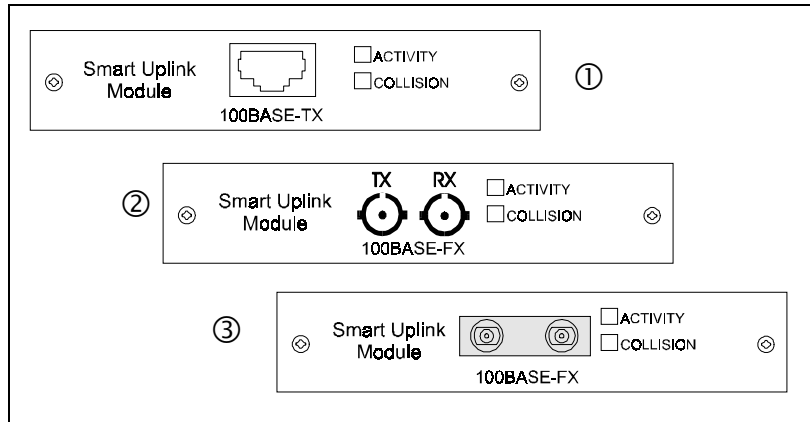


Figure 3- 3. Smart Uplink Modules

NOTE: The Smart Uplink Module port is the 25th logical port on the hub.

Inserting the Smart Uplink Module into the Smart Uplink Slot

To insert a Smart Uplink Module into a Netelligent 2724 or 2824 Smart Uplink slot, follow these steps:

1. Power down the hub by disconnecting the power cord from the power source.

3-4 Installing the Hub

2. Remove the Smart Uplink port cover plate from the hub's front panel.
3. Insert the Smart Uplink module through the port hole, aligning the sides of the SUM with the card guides inside the hub (Figure 3-4).

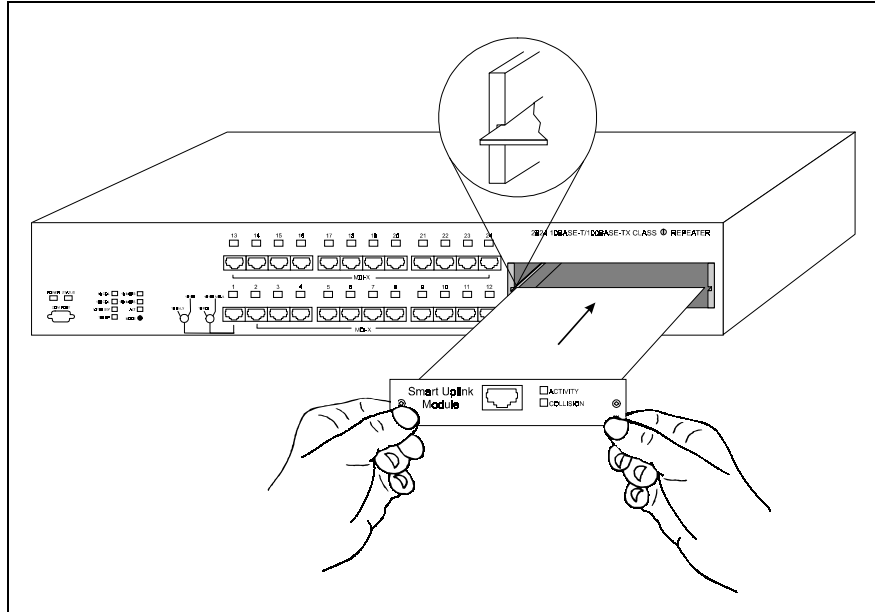


Figure 3- 4. SUM Installation

4. Carefully push the Smart Uplink module's 50-pin male connector into the SUM socket on the hub motherboard until the SUM is firmly seated and its faceplate is flush with the hub's front panel.



CAUTION: Do not tighten the Smart Uplink Module's spring screws until completing Step 4 of this procedure. If you tighten the spring screws before the SUM is properly seated in the socket, you may damage the hub.

5. Secure the SUM to the hub by tightening the SUM's spring screws.

Connecting Cable

Each RJ-45 port on the hub can accept a standard 8-wire twisted-pair (UTP) cable that ends with RJ-45 connectors. This type of cable can be up to 100 meters (328 feet) in length.

A 100Base-FX port on a SUM can accept multi-mode 62.5/125 to 100/150 micron fiber cable that ends with fiber SC-type connectors. This type of cable can be up to 2 Km in length at full-duplex operation.

To attach the cable, plug one of the cable connectors into the selected port on the hub. Connect the other end of the cable to the corresponding port on a 10Base-T, 100Base-TX, or 100Base-FX workstation (if you installed a 100Base-FX SUM).

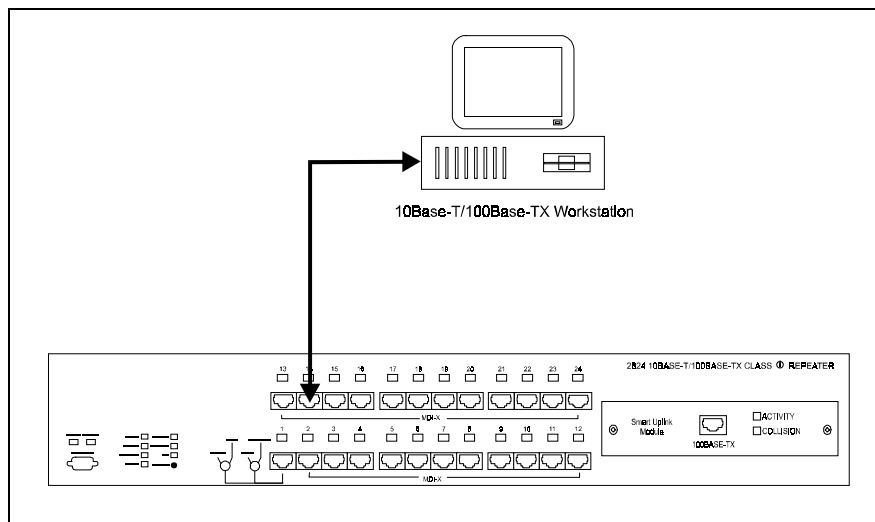


Figure 3- 5. Connecting Twisted-Pair Cable to an RJ-45 Port

Interconnecting Hubs

You can interconnect two manageable 2724 hubs to create an unmanaged stack. Or, you can interconnect up to four manageable 2724 hubs with one managing 2824 hub for a fully managed stack. You can also interconnect the 2724 and 2824 hubs with Netelligent 2524 (manageable) and 2624 (managing) hubs.

NOTE: Only one managed hub (2824 or 2624) is allowed in a single stack.



CAUTION: It is recommended that you power down the 2724/2824 stack before you add another hub to the stack. Adding a hub with the stack powered on could create unpredictable results.

You can place the 2824 hub in any position (top, middle, bottom) in a two- to five-hub stack. The 2824 hub has an expansion interface that consists of four 68-pin backplane connection cables (EXPN PORT A, B, C, and D) on the hub's back panel.

The 2724 hub has one 68-pin backplane connection cable (EXPN PORT) and three dip switches for UNM/MAN, HOST/TARGET, and SW EN/SW DIS settings. The switch settings are described in the section “2724 Dip Switch Settings” in this chapter.

If possible, mount the hubs on a rack or place them on a stable mounting surface with the supplied rubber feet affixed before you attach the backplane connection cable. This helps ensure the correct spacing between hubs and helps prevent stretching and possibly damaging the backplane connection cable during installation.

2724 Dip Switch Settings

The dip switches on the back of the 2724 hub come factory pre-set so that you can create a *managed* stack of up to five hubs (one to four 2724 hubs and one 2824 hub). Or, by reconfiguring the dip switches, you can create an *unmanaged* stack of two 2724 hubs. The dip switch settings are described below:

IMPORTANT: Incorrectly setting the dip switches will not damage the hubs, but may affect switch management.

HOST/TARGET

- **TARGET** — (Factory default setting) Lets you connect one, two, three, or four 2724 hubs to a 2824 managing hub to form a “managed” dual-speed hub.
- **HOST** — Lets you connect two 2724 hubs in an *unmanaged* stack to form a single 48-port dual-speed hub (with no 2824 hub in the stack). One hub must be re-configured as the HOST and the other as the TARGET.

Invalid Connections

The following are invalid connections for the 2724/2824 hubs:

- Connecting two 2824 managing hubs together — Hubs will operate as if disconnected.
- Setting a 2724 hub in a managed stack to the HOST mode — Hubs will operate as if disconnected. The STATUS LED is always off in an unmanaged stack. To correct this condition, set the DIP switch on the 2724 hub to TARGET.
- Setting both 2724 hubs in an unmanaged stack to HOST or to the TARGET mode — The STATUS LED is always off in an unmanaged stack. To correct this condition, set the DIP switch on one hub to HOST and set the DIP switch on the other hub to TARGET.

UNM/MAN

- **UNM (Unmanaged)** — In this mode, if you change the DIP switch on the 2724 hub to UNM, all hub ports on the 2724 are automatically enabled after turning the hub off and then back on. This mode lets you use a 2724 under the following conditions:
 - The 2724 is disconnected from the 2824.
 - The 2824 is off or otherwise not operating.

- **MAN (Managed)** — (Factory-default setting) In this mode, the port configuration settings for the 2724 hub are non-volatile. In addition, if you remove the 2724 hub from the stack, the disabled ports remain disabled. (You can re-enable them by setting the DIP switch to UNM and turning the hub off and then back on.) For example, if you disable Ports 1 and 2, then power down the stack, Ports 1 and 2 will still be disabled when the stack is powered up again.

In a managed stack, if you set the 2724 DIP switch to UNM, the STATUS LED on the 2724 flashes GREEN.

Figure 3-6 shows two expansion ports of a 2824 hub connected to the expansion ports of two 2724 hubs using backplane connection cables.

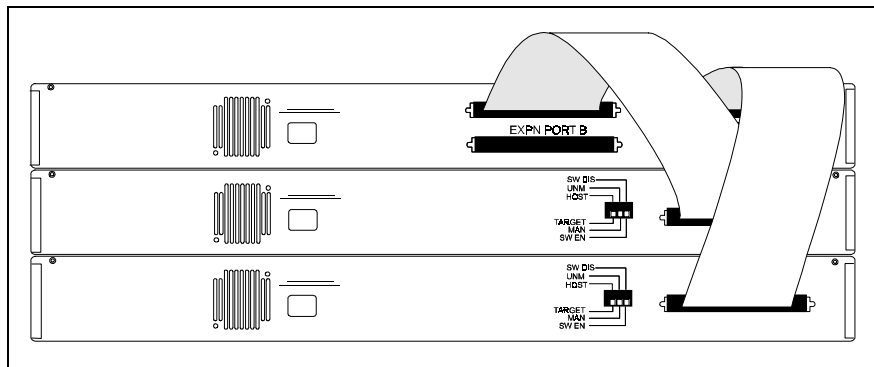


Figure 3- 6. Stack Connecting One 2824 and Two 2724 Hubs with Backplane Connectors

In this example, the 2824 hub (top hub in the stack) manages two 2724 hubs. The DIP switches on both 2724 hubs are set to “TARGET,” as required in a managed stack.

Figure 3-7 shows two 2724 hubs connected via a backplane connector between the EXPN PORTs. The DIP switches on the 2724 hubs are set with the top hub as the HOST and the bottom hub as the TARGET.

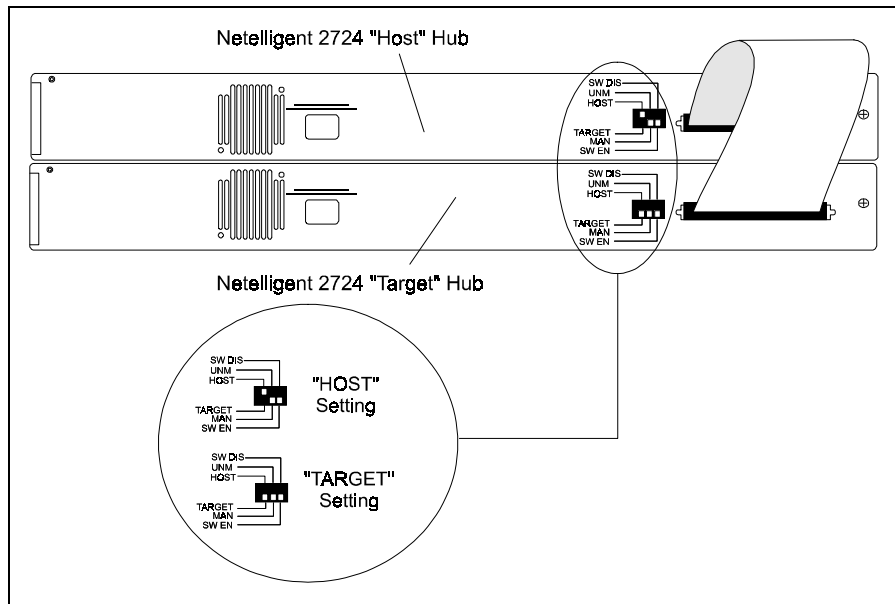


Figure 3- 7. Interconnecting Two 2724 Hubs Via a Backplane Connection Cable

In this example, the unmanaged stack consists of the maximum of two 2724 hubs. Either hub in the stack can be the HOST or the TARGET. Both hubs are in the factory-default MAN mode.

Connecting Power

Follow these steps to connect the hub to power:

1. Plug the power cord into the power connector on the back of the hub.
2. Insert the three-pronged plug on the power cord into a non-switched grounded power source. The power source should be near the hub and easily accessible.

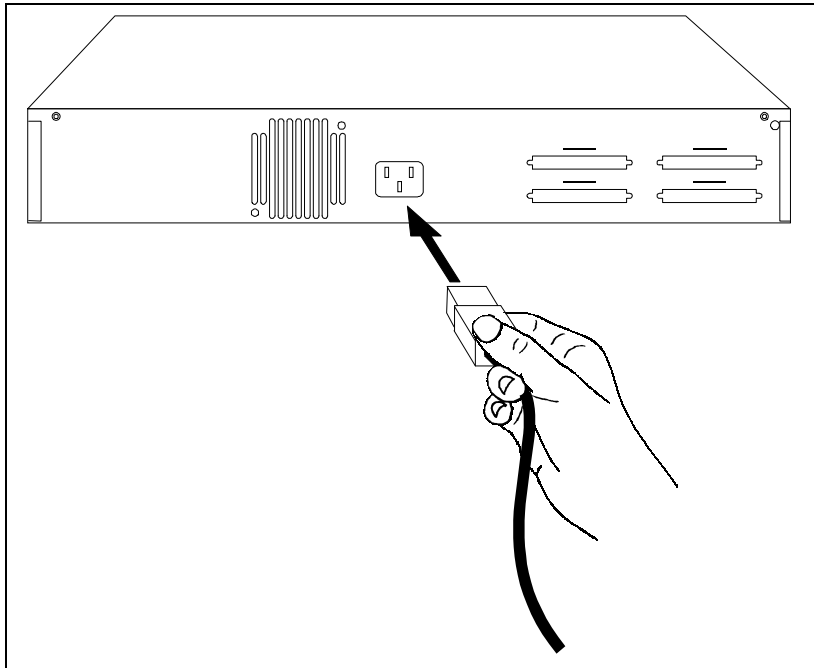


Figure 3- 8. Connecting the Power Cord

When you plug in the power cord, the hub performs a self test in which the RJ-45 LEDs are green (or yellow if collisions are occurring), off, yellow, and off again. Each state is about ½ second in duration. After the test, the POWER LED lights steady green.

Disconnecting Power

To power down the hub, disconnect the power cord from the power source. Do not power down the hub by disconnecting the power cord from the back of the hub.

Connecting to the Serial Port

To enable management of the hub, you must first set its IP address (See Chapter 4 – “Setting the IP Address”). One way to set the IP address is through the hub's built-in VT100 interface. To use this interface, you must connect a workstation to the hub's serial port using a null modem (to set the IP address locally) or to a regular modem (to set the IP address remotely). The serial cable has a DB-9 connector at each end. Figure 3-9 shows a connection to a workstation using a null modem. Figure 3-10 shows an Example of a connection to a workstation via a regular modem.

3-12 Installing the Hub

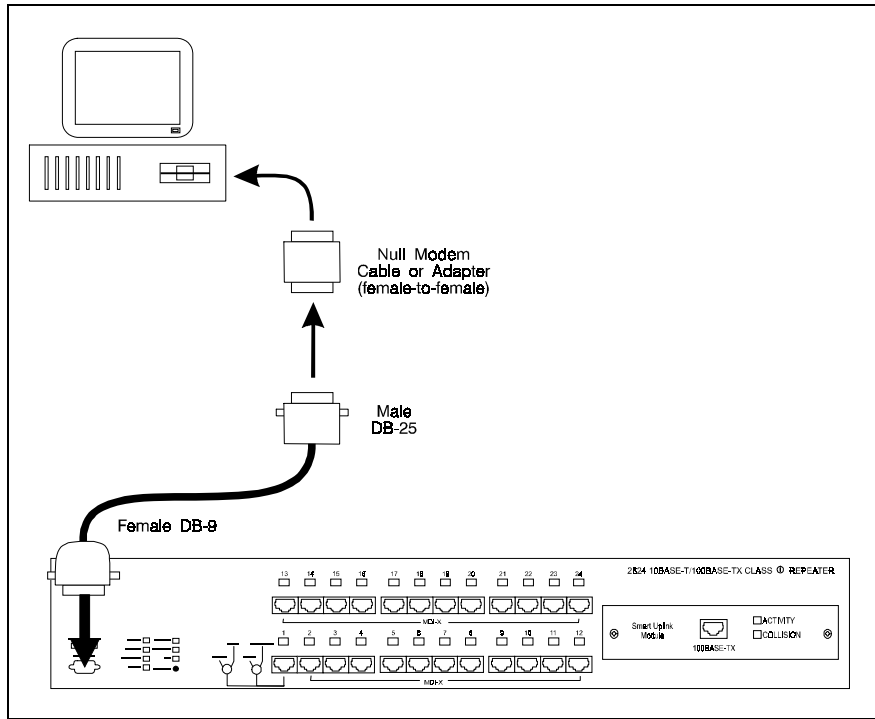


Figure 3- 9. Local Connection via Null Modem

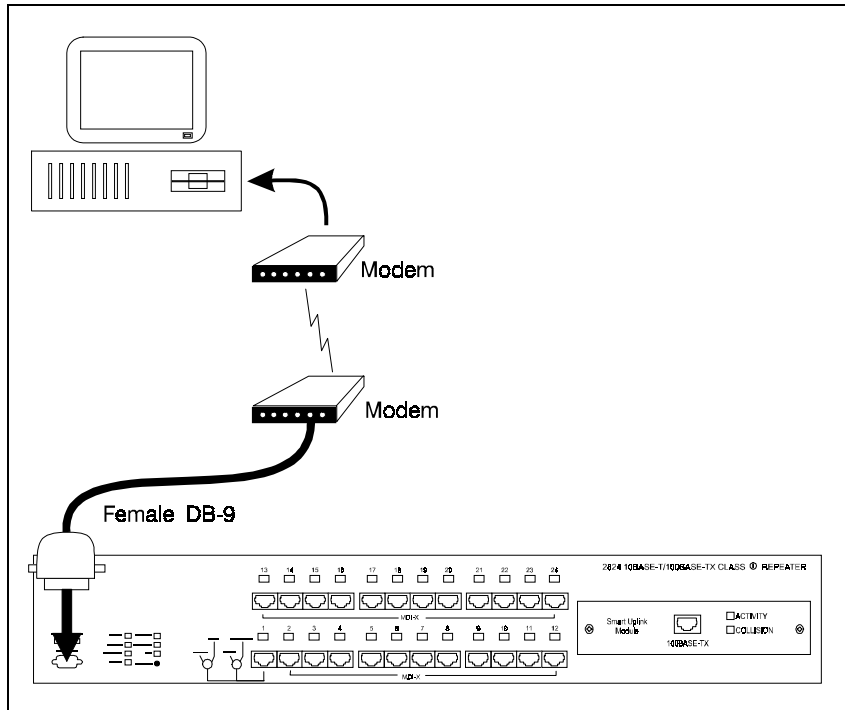


Figure 3- 10. Remote Connection via Regular Modem

Chapter 4

Configuring the Hub for Management

To allow management of the 2824 hub, you must first set its IP address. After you set the IP address, you can set additional configuration parameters using the VT100 interface discussed in Appendix A “Using the VT100 Interface.” Or, you can manage the hub using Compaq Netelligent Management Software, which is included on CD with the hub.

Setting the IP Address Using VT100

The following procedure describes how to initially set the IP address using Windows 95 HyperTerminal. However, the settings described in these steps apply to any terminal emulation application. After you set the IP address the first time, you can change the address using the VT100 interface, Netelligent Management Software, or other SNMP management application. Follow these steps to set the IP address using VT100.

NOTE: You can also set the IP address using a BOOTP server. See “Setting the IP Address Using a BOOTP Server” at the end of this chapter.

1. Connect the modem as described in “Connecting a Modem” in Chapter 3 “Installing the Hub.”
2. Start the terminal emulation program.

.....

4-2 Configuring the Hub for Management

3. Type a name for the connection (for example, "IP Setup") and click on OK.

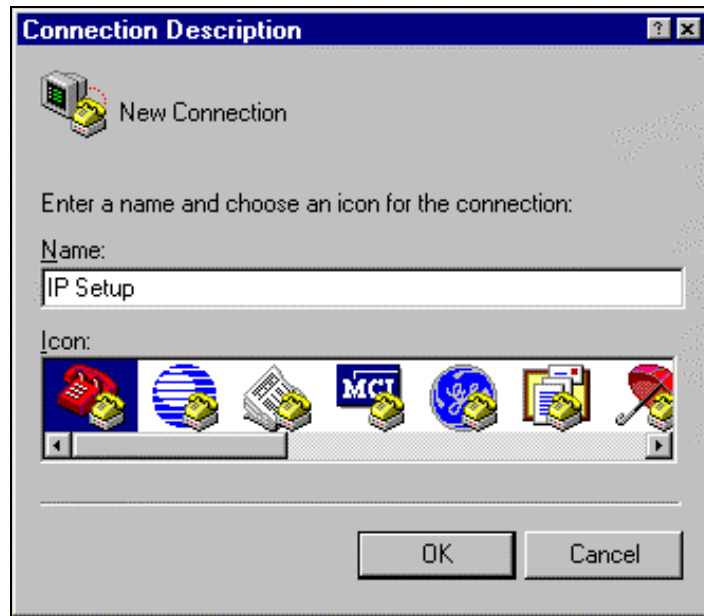


Figure 4- 1. Connection Description Screen

4. Select the *Direct to Com 1* option (in this example) in the *Connect using* field of the *Phone Number* dialog box. Click on OK.
-



Figure 4- 2. Phone Number Dialog Box

5. Enter the following port settings in the dialog box and click on OK.
 - Bits per second: 9600
 - Data bits: 8
 - Parity: None
 - Stop bits: 1
 - Flow control: None

4-4 Configuring the Hub for Management

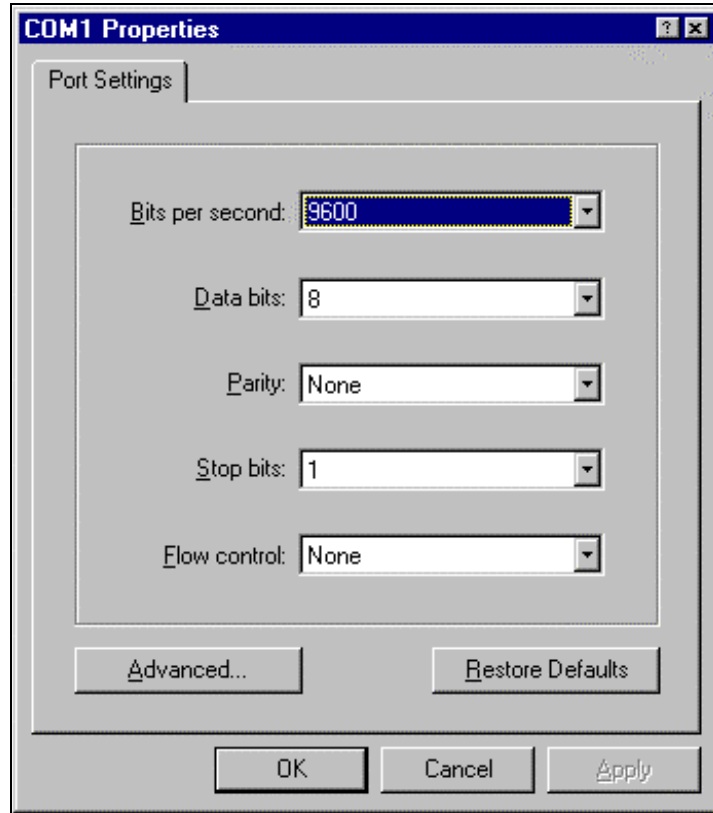


Figure 4- 3. COM1 Properties Dialog Box

6. Enter the following command:

```
vt100
```

The Login screen appears.

NOTE: If the login fails, you may need to retry the connection several times.

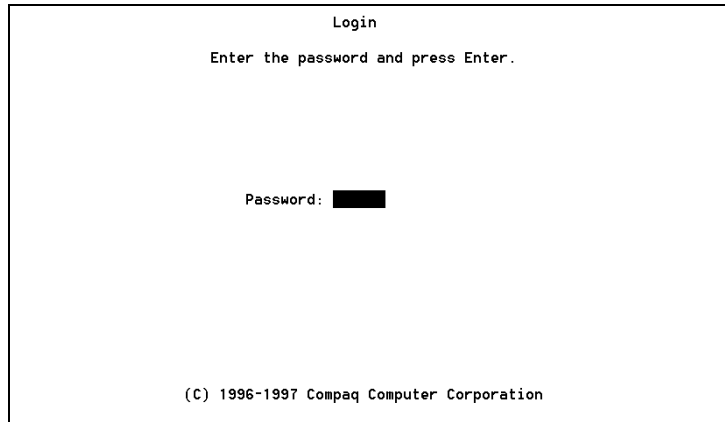


Figure 4- 4. Login Screen

7. Within 20 seconds after the Login screen appears, type and enter the word “public,” which is the default password. The Main menu screen appears.

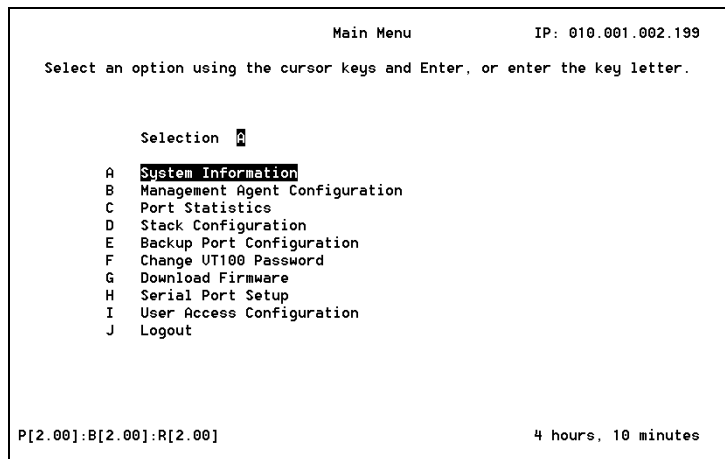


Figure 4- 5. Main Menu Screen

4-6 Configuring the Hub for Management

8. Highlight Option B, Management Agent Configuration, using the down arrow key or <Tab> key. Then press <Enter>. The Management Agent Configuration screen appears.

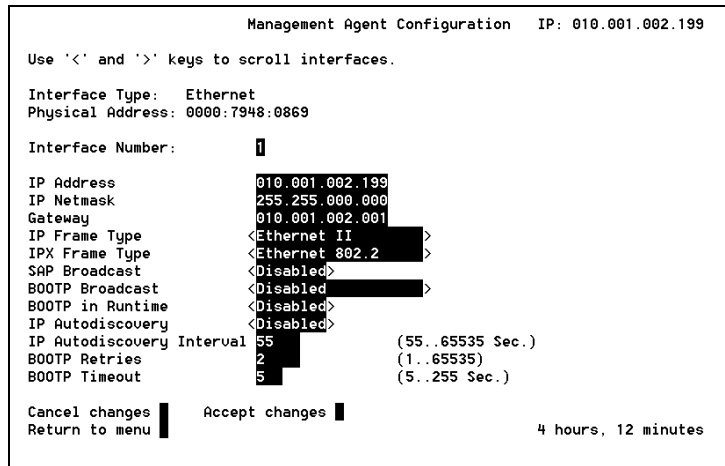


Figure 4- 6. Management Agent Configuration Screen

9. Use the arrow or tab keys to move to the IP Address field. Then enter the IP address for the Ethernet interface. To set the IP address for other interfaces (for example, SLIP), use the "<" and ">" keys to scroll to group and repeat this step.
10. Move the cursor to the Accept Changes field and press <Enter>. Then move the cursor to the Return to menu field and press <Enter>.
11. Select Option J (Logout) to log out of the VT100 session.

You can change the initialization string using the Modem Setup screen of the VT100 interface. For example, you could set the string as "Enter VT100 now" to provide a more instructive cue to enter the VT100 command. You can also change the password to log in to VT100 using the Change Password screen. For a complete description of the VT100 interface, see Appendix B "Using the VT100 Interface."

Setting the IP Address Using a BOOTP Server

You can configure a BOOTP server to supply the IP address, subnet mask, and gateway IP address for the hub. Once the BOOTP server is configured with the desired settings, it automatically configures the hub in response to the hub's BOOTP requests.

The 2824 hub has two boot phases: Boot and Runtime. In the Boot phase (STATUS LED is orange), the hub issues as many requests as are defined in the *cpqnBootpRetries* MIB object. The default number of requests is two. The hub issues the requests using two different frame types (Ethernet_II and 802.2 SNAP). The interval between requests is defined in the *cpqnBootpRetryInterval* MIB object. The default request retry interval is 5 seconds. In the Runtime phase (STATUS LED is green) and when BOOTP requests are enabled and the hub does not have an IP address currently assigned, the hub issues requests every 5 minutes using only one frame type (same as the IP frame type). If the hub receives a response from the server, it uses the information to configure itself accordingly.

You can use Compaq Netelligent Management Software (or other SNMP network management application) or the hub's VT100 interface to disable BOOTP requests by setting the *cpqnBootEnable* MIB object to `disable-bootp(1)`. This is recommended if you use only IPX communication, as it helps reduce unnecessary traffic generated by the hub.

Chapter 5

Managing the Hub

This chapter discusses the management functions of the Netelligent 2824 hub.

Management Features

The 2824 hub has the following management features:

- Support for SNMP, VT100, and Compaq Netelligent Management Software management applications
- Four-group Remote Monitoring (RMON)
- Firmware upgrade capabilities

Management Interface

After you set the IP address for the 2824 hub (described in Chapter 4, “Configuring the Hub for Management”), you can use BOOTP, VT100, SNMP, or Compaq Netelligent Management Software to configure the network parameters and manage the hub. Each of these methods varies in the management functions it can perform. The following table lists network configuration parameters and the various management interfaces you can use to modify them.

Network Configuration Parameters and Modification Methods				
Network Configuration Parameters	Modification Methods			Default Parameter Setting
	BOOTP	VT100	SNMP	
IP address	✓	✓	✓	0.0.0.0
IP network mask	✓	✓	✓	Derived from IP address
IP gateway	✓	✓	✓	0.0.0.0
SLIP IP address		✓	✓	0.0.0.0
SLIP IP network mask		✓	✓	Derived from SLIP address
SLIP IP gateway		✓	✓	0.0.0.0
IPX address				IPX network of requester + MAC address
BOOTP request enable		✓	✓	Enabled
BOOTP retries		✓	✓	2
BOOTP retry interval		✓	✓	5 seconds
IP frame type		✓	✓	Ethernet II
IPX frame type		✓	✓	Ethernet 802.2
IP autodiscovery enable		✓	✓	Enabled
IP autodiscovery ping interval		✓	✓	55 seconds
SAP broadcast		✓	✓	Enabled
IP trap receivers			✓	None
IPX trap receivers			✓	None

Table 5-1 . Network Configuration Parameters and Modification Methods

SNMP Management

The 2824 hub supports SNMP management through both in-band and out-of-band communications. In-band management support is provided by SNMP over IP and IPX protocol stacks and VT100 emulation over Telnet (TCP/IP). Out-of-band management support is provided by SNMP over SLIP and through direct serial interfaces using VT100 emulation. The 2824 hub stores management configuration information in Non-Volatile RAM (NVRAM), which helps protect the configuration from a power outage. See “Parameters Stored in NVRAM.”

Supported MIBs

The 2824 hub supports the following standard MIBs under SNMP, which determine what management functions it can perform:

- RFC1213 (MIB II) — Management Information Base for Network Management of TCP/IP-based Internets (MIB II)
- RFC1516 — Definitions of Managed Objects for the IEEE 802.3 Repeater Devices (technically part of MIB II)
- RFC1757 (RMON) — Remote Network Monitoring Management Information Base (RMON MIB)
- HUBNVLE — Novell Ethernet Repeater MIB
- CPQN2FE — Compaq Netelligent 2000 Fast Ethernet MIB
- CPQNUNIF — Compaq Netelligent Unified MIB

Supported Frame Types

The hub supports four different Ethernet frame types. It is important to know that the 2824 hub supports the frame types used in your network. For convenience, each frame type is referred to by its Novell name. The following table lists each frame type, its Novell name, and whether or not it is supported for IP and IPX.

Supported Frame Types			
Ethernet Frame Type	Novell Name	IP	IPX
"DIX" Ethernet II	ETHERNET_II	✓	✓
IEEE 802.3 with 802.2 SNAP Headers	ETHERNET_SNAP	✓	✓
IEEE 802.3 with 802.2 LLC Headers	ETHERNET_802.2		✓
IEEE 802.3 "Raw"	ETHERNET_802.3		✓

IP Frame Types

The hub supports both ETHERNET_II and ETHERNET_SNAP for its Ethernet IP communications. The default frame type is ETHERNET_II. However, many networks composed of FDDI, token ring, and Ethernet topologies require the ETHERNET_SNAP frame type for routing, bridging, and switching. To provide IP management flexibility, the 2824 hub supports both ETHERNET_II and ETHERNET_SNAP frame types.

Although the hub supports two different Ethernet frame types, it cannot support both simultaneously. This is because an individual IP network can only use one frame type and different frame types require different IP networks even if they run on the same cable.

The hub's IP frame type can be set by three different methods:

- BOOTP — Sends requests over ETHERNET_II and/or ETHERNET_SNAP frame types, which you can configure, as needed. The hub's IP frame type is set to the frame type of the BOOTP response (if it is received) and saved in non-volatile memory.

NOTE: If the hub transmits BOOTP requests over two frame types, this lengthens the time required to complete the BOOTP process.

- SNMP — If you set the frame type using SNMP over IP, you must set the IP address using the *cpqnIpAddr* MIB variable. SNMP over IPX does not require an IP address configuration.
- VT100 — You can set the hub's IP frame type from the Management Agent Configuration screen. The 2824 hub saves changes in non-volatile memory.

NOTE: If you are using Telnet or SNMP over IP, the hub must already have a valid configuration for either its IP or SLIP interface.

To determine which IP frame type it will implement, the hub uses the following priority scheme:

- If a BOOTP response is received during the BOOTP process, uses the frame type of the received packet
- If no BOOTP response is received during the BOOTP process, uses the frame type saved in non-volatile memory
- If no value is stored in non-volatile memory, uses the default value of ETHERNET_II

At any time after the initial BOOTP process, you can change the frame type using VT100 or by setting the MIB object *cpqnIpFrameType*.

IP Protocols

The hub supports the following IP protocols:

UDP (User Datagram Protocol)	Provides non-guaranteed delivery service over IP. The hub implements a full UDP stack. Supports IP fragmentation maximum packet size of 1520 bytes.
ARP (Address Resolution Protocol)	Allows discovery of the hardware address associated with a given IP address
ICMP (Internet Control Messages Protocol)	Provides error and control messages. A Ping packet is a type of ICMP packet.
SNMP (Simple Network Management Protocol)	Allows management of a network node by another node. The hub provides full support of SNMP and implements several standard MIBs as well as product-specific MIBs.
BOOTP (Boot Protocol)	Allows a network node to automatically obtain its IP configuration from a central BOOTP server; an alternative to individually configuring each node. Also used to trigger a TFTP firmware download.
TFTP (Trivial File Transfer Protocol)	Supported for firmware upgrades
TCP (Transmission Control Protocol)	Provides guaranteed delivery service over IP. It is required for Telnet support.
Telnet	Provides terminal emulation over a network. This is the VT100 interface.

IP Autodiscovery

The hub supports a generic IP autodiscovery method used by many of the leading SNMP management platforms (such as HP OpenView, SunNet Manager, IBM NetView 6000). This method lets the management platforms automatically discover managing 2824 hub in the network.

Generic IP autodiscovery works by looking at the addresses cached by routers and gateways. These caches are periodically flushed. For a node to remain in the gateway's cache, it must transmit at least as often as the cache is flushed.

The 2824 hub implements IP autodiscovery via two MIB objects, each of which is stored in non-volatile memory.

MIBs Implementing IP Autodiscovery

MIB Object	Function
cpqnlpPingPktRate	Sets the rate of ping transmissions so that it can match the IP gateway's cache aging timer, preventing the 2824 hub from being deleted from the ARP cache. If you do not configure a default IP gateway (set through either SNMP or VT100 management interfaces), the hub does not transmit the periodic ICMP Pings and cannot guarantee IP autodiscovery. Default – 55 seconds.
cpqnlpAutoDiscoveryStatus	Disables or enables IP autodiscovery. Default = <i>discover(1)</i>

IPX Frame Type

In addition to IP, the 2824 hub also supports an IPX protocol stack. To provide seamless network management, all Ethernet frames types supported by Novell must be supported by hubs. The firmware supports the following frame types for IPX:

- ETHERNET_II
- ETHERNET_802.3
- ETHERNET_802.2
- ETHERNET_SNAP

IMPORTANT: Since Novell uses ETHERNET_802.2 as the default frame type for IPX, the default IPX frame type of the hub is also ETHERNET_802.2.

Most IPX communications uses IPX packets that are initiated by a requestor, not the hub. A management station sends these packets to the hub and waits for a response. The hub receives the packet and sends it back using the same frame type and IPX network number used to send the packet. For response traffic, therefore, the hub supports all IPX frame types.

In addition, the hub originates some types of IPX traffic, such as packets for SNMP traps and RIP and SAP broadcasts. Consequently, to transmit the packet, the hub must know the IPX frame type and network number. This requires the use of MIB variables, one of which is the IPX frame type variable.

To determine which IPX frame type it will implement, the hub uses the following priority scheme:

- Uses the value stored in NVRAM
- If no value is stored in NVRAM, uses the default value of ETHERNET_802.2

You can change the frame type at any time by setting the IPX frame type MIB variable through the VT100 interface, SNMP, or Compaq Netelligent Management Software.

The IPX network numbers for SNMP traps are determined through the MIB variables indicating the IPX trap receiver addresses. IPX network numbers for RIP and SAP broadcasts are learned by analyzing the RIP broadcasts sent from IPX routers on the network. If the network number cannot be learned through the network traffic, the default network number 0 is used.

IPX Protocols

The hub supports the following IPX protocols:

IPX Protocol	Function
SNMP (Simple Network Management Protocol)	Functions the same as SNMP over IP. All SNMP features available over IP are available over IPX. Novell's ManageWise uses SNMP over IPX to manage HMI hubs, which the hub emulates.
IPX Diagnostics	Allows a node to report which IPX functions it supports. The hub supports IPX Diagnostics to be compatible with Novell's NetExplorer server, a part of ManageWise.
SAP (Service Advertising Protocol)	<p>Allows a node to advertise which IPX services it supports. The hub advertises two services:</p> <ul style="list-style-type: none"> • HMI services (SAP ID 0x0239) — Causes ManageWise to recognize the hub as a manageable repeater • Netelligent services (SAP ID 0xAF05)— Can be used to select an icon for display on the ManageWise segment map <p>NetWare servers store the available service in the Bindery from which other servers and management applications, such as ManageWise, can query it.</p>
RIP (Routing Information Protocol)	Allows IPX nodes to exchange routing information. The hub uses RIPs to determine the IPX number(s) and Ethernet frame type(s) of its local segment; determines how to route SNMP/IPX traps; and supports IPX autodiscovery.

IPX Autodiscovery

The hub supports Novell IPX autodiscovery through its HMI-compliance mechanism so that management platforms, such as Novell's ManageWise, can automatically discover managing hub. The protocols involved in IPX autodiscovery support are SAP, RIP, and IPX Diagnostics.

Using SAP, the hub advertises that it is an HMI server (although not all of the server functions are implemented). This registers the hub in the Binderies of all the NetWare servers on the network segment. When Novell's NMS or ManageWise initiates autodiscovery, it queries the Binderies of all the servers it knows to obtain the internal IPX address of HMI servers. ManageWise then uses RIP to obtain the hub's MAC address and other information required to start SNMP/IPX management.

IPX Diagnostics are implemented only to support the NetExplorer server. This protocol is not directly involved with the IPX autodiscovery algorithm, but is used to update the ManageWise database with the current network configuration.

NetWare servers age out Bindery entries after 60 seconds. To remain in a server's Bindery and stay available for autodiscovery by ManageWise, the hub broadcasts SAPs every 55 seconds. You can disable this feature by setting the MIB object *cpqnIpxSAPBcastStatus* to *no-ipx-SAPs(2)*. The value of this object is stored in non-volatile memory.

SLIP Protocols

The 2824 hub uses SLIP (Serial Line IP) to provide remote, out-of-band management through the serial port. The same IP protocols supported over Ethernet are also supported over SLIP, including SNMP and Telnet.

IP fragmentation is supported over SLIP. Fragmentation allows the hub to receive the same maximum IP packet size, 1520 bytes, for both SLIP and Ethernet. The maximum packet size over SLIP is 1006 bytes.

To establish a SLIP connection, you must set the IP address and the subnet mask for the SLIP interface, using the VT100 interface or SNMP management.

Traps

To receive a trap, the SNMP network management station must place its IP or IPX address into the appropriate trap destination table of the Netelligent Unified MIB (CPQNUNIF). The trap destination tables are listed below:

- For IP traps, the destination table is *cpqnIpTrapDestTable*
- For IPX traps, the destination table is *cpqnIpxTrapDestTable*

Each IP and IPX trap tables can contain a maximum of ten entries.

The table below summarizes the traps generated by the hub. The headings are defined as follows: *MIB* is the MIB or RFC that defines the traps. *Trap* lists the traps by a convenient name. *RFC1157 Trap Type* lists the RFC1157 generic trap category to which the trap belongs; for *enterpriseSpecific* traps, the enterprise and trap numbers are also shown. *Variable Bindings* lists the additional MIB objects included in the trap message.

Generated Traps			
MIB	Trap	RFC1157 Trap Type	Variable Bindings
RFC1157	Cold Start	<i>coldStart(1)</i>	(none)
	Authentication Failure	<i>authenticationFailure(4)</i>	(none)
RFC1757 (RMON)	Rising Alarm	<i>enterpriseSpecific(6): rmon.1</i>	<i>alarmIndex, alarmVariable, alarmSampleType, alarmValue, alarmRisingThreshold</i>
	Falling Alarm	<i>enterpriseSpecific(6): rmon.2</i>	<i>alarmIndex, alarmVariable, alarmSampleType, alarmValue, alarmFallingThreshold</i>
RFC1516**	Health	<i>enterpriseSpecific(6): snmpDot3RptrMgt.1</i>	<i>rptrOperStatus, rptrHealthText</i>
	Group Change	<i>enterpriseSpecific(6): snmpDot3RptrMgt.2</i>	<i>rptrGroupIndex</i>
	Reset	<i>enterpriseSpecific(6): snmpDot3RptrMgt.3</i>	<i>rptrOperStatus</i>

5-12 Managing the Hub

HUBNVLE* *	Health	<i>enterpriseSpecific(6): nSnmpDot3RptrMgt.1</i>	<i>rptrBasHealthState, rptrBasHealthText, rptrBasHealthData, rptrBasID, rptrExtName</i>
	Group Change	<i>enterpriseSpecific(6): nSnmpDot3RptrMgt.2</i>	<i>rptrBasGroupMap, rptrBasId, rptrExtName</i>
	Reset	<i>enterpriseSpecific(6): nSnmpDot3RptrMgt.3</i>	<i>rptrBasHealthState, rptrBasHealthText, rptrBasHealthData, rptrBasID, rptrExtName</i>

** RFC1516 traps and HUBNVLE traps are issued under the same circumstances. Because of this, the hub issues traps from one or the other MIB, but not both. The CPQN2FE MIB variable *n2feTrapSupport* lets you select which traps are issued.

The following table describes when the 2824 hub issues each trap. The Health, Group Change, and Reset traps are listed only once since they are issued under the same circumstances.

Traps Issued	
Trap	Issued When
Cold Start	Issued when the hub has completed a re-initialization
Authentication Failure	Issued when the hub receives an SNMP request that is not “properly authenticated”; usually this indicates an invalid community string
Rising Alarm	Issued when a monitored MIB object exceeds a specified threshold. The <i>RMON alarmTable</i> and <i>eventTable</i> must be appropriately configured to enable this trap.
Falling Alarm	Issued when a monitored MIB object falls below a specified threshold. The <i>RMON alarmTable</i> and <i>eventTable</i> must be appropriately configured to enable this trap.
Health	Issued when changes occur in the 2824 hub operational state
Group Change	Issued when a unit is added or removed from the stack. The RFC1516 trap provides the unit number whose status changed. In the HUBNVLE trap, a 16-bit bitmap shows which units are currently present in the stack; the least significant bit represents unit 1.
Reset	Issued after completion of a reset initiated by <i>rptrReset</i> or <i>rptrBasReset</i>

RMON Support

Remote monitoring (RMON) lets a management system remotely monitor and report network activity. Of the nine groups defined by RMON in RFC1757, the 2824 hub implements four, including Statistics, History, Alarm, and Event. RMON is designed to supplement the management information from SNMP. In particular, RMON provides functions for getting information about the operation and performance of entire networks or of subnetworks in an internetwork.

Statistics Group

The statistics group, as defined in RFC1757, consists of the Ethernet Statistics Table (*etherStatsTable*). This table contains objects that report normal traffic and error counts. It can evaluate the network load on a data source. Statistics monitors are listed below.

etherStatsDropEvents	etherStatsOctets
etherStatsPkts	etherStatsBroadcastPkts
etherStatsMulticastPkts	etherStatsCRCAlignErrors
etherStatsUndersizePkts	etherStatsOversizePkts
etherStatsFragments	etherStatsJabbers
etherStatsCollisions	etherStatsPkts64Octets
etherStatsPkts65to127Octets	etherStatsPkts128to255Octets
etherStatsPkts256to511Octets	etherStatsPkts512to1023Octets
etherStatsPkts1024to1518Octets	

RMON collects statistics for any data source and can monitor multiple data sources.

History Group

The history group tracks the network load over a period of time. The history group consists of the History Control Table (*historyControlTable*) and the Ethernet History Table (*etherHistoryTable*). The *historyControlTable* defines the way in which samples are taken and specifies the data source, the polling interval, and the number of samples (“buckets”) to store. The *etherHistoryTable* stores these “buckets” of sampled data, which consist of the following MIB objects:

etherHistoryIntervalStart	etherHistoryDropEvents
etherHistoryOctets	etherHistoryPkts
etherHistoryBroadcastPkts	etherHistoryMulticastPkts
etherHistoryCRCAlignErrors	etherHistoryUndersizePkts
etherHistoryOversizePkts	etherHistoryFragments
etherHistoryJabbers	etherHistoryCollisions
etherHistoryUtilization	

For each entry in the *historyControlTable*, RMON takes samples until the entry is deleted. If RMON takes more samples than there are buckets, RMON “recycles” the entry’s “buckets” for the *etherHistoryTable*. This means that the last N samples are stored, where N is the number of buckets. However, when buckets are “recycled”, their indices are not renumbered; the hub continues assigning indices to samples. Thus it is possible for the first sample in an *etherHistoryTable* entry to start with a number other than 1.

The 2824 hub saves the parameters in the *historyControlTable* in NVRAM and restores these parameters each time the hub is re-initialized. However, the 2824 hub does not save the sampled data from the *etherHistoryTable*.

Alarm Group

The alarm group provides a means of generating an “alarm” when a specified MIB variable exceeds a specified threshold. Each alarm is associated with an “event” defined in the RMON Event group. The same event can trigger multiple alarms. An RMON “event” can be used with the RMON Event group to issue notifications (such as SNMP traps) to the user.

The alarm group consists of the Alarm Table (*alarmTable*). Each entry in the table defines a MIB object to monitor, how often to monitor it, and the thresholds of the MIB object’s value that cause an event to be generated. The 2824 hub stores *alarmTable* entries in NVRAM and restores these each time the hub is re-initialized. When an *alarmTable* entry is created, the *alarmRisingThreshold* and *alarmFallingThreshold* objects are set to 0. The Alarm group consists of the following MIB objects:

<i>alarmInterval</i>	<i>alarmVariable</i>
<i>alarmSampleType</i>	<i>alarmValue</i>
<i>alarmStartupAlarm</i>	<i>alarmRisingThreshold</i>
<i>alarmFallingThreshold</i>	<i>alarmRisingEventIndex</i>
<i>alarmFallingEventIndex</i>	<i>alarmOwner</i>
<i>alarmStatus</i>	

The *alarmTable* can generate two types of alarms: a *rising* alarm and a *falling* alarm. These alarms can result in SNMP traps if the alarm’s associated event in *eventTable* is configured to generate traps.

The following conditions allow the generation of rising-alarm events:

1. If the first sampled value obtained after the [*alarmTable*] row becomes valid is:
 - a. less than the rising threshold, then the first time that the sample value becomes greater than or equal to the rising threshold, a rising-alarm event is generated.

- b. greater than or equal to the rising threshold, and if the value of `alarmStartupAlarm` is `risingAlarm(1)` or `risingOrFallingAlarm(3)`, then a rising-alarm event is generated.
 - c. greater than or equal to the rising threshold, and if the value of `alarmStartupAlarm` is `fallingAlarm(2)`, then a rising-alarm event is generated after having fallen below the rising threshold.
2. After a rising-alarm event is generated, another such event will not be generated until after the sampled value falls below the rising threshold and reaches the falling threshold and then subsequently reaches the rising threshold again.

The conditions for the generation of falling-alarm events are the reverse of those listed above.

The number of *alarmTable* entries that may be configured is limited by the agent's RAM and NVRAM resources.

Event Group

The Event group controls the generation of event notifications. An event notification can be an SNMP trap and/or an entry in an event log. In the 2824 hub, the only triggers of events are alarms defined in the Alarm Table. In other words, an alarm can trigger an event, which can then issue a notification.

The event group is composed of the Event Table (*eventTable*) and the Log Table (*logTable*). Each entry in *eventTable* specifies a set of notification parameters. Multiple conditions may trigger a single event notification. The *logTable* stores event notifications for those events that create a log entry.

The notification parameters specified by the *eventTable* entries are saved in NVRAM and are restored each time the hub is re-initialized. The event log stored in *logTable*, however, is not saved.

When an event generates a trap, the community for the trap message is taken from the associated *eventTable* entry's *eventCommunity* object. The condition that triggered the event determines the enterprise and specific trap fields.

Firmware Updates

You can update the firmware for the 2824 hub with several file transfer methods:

Firmware Update Methods			
File Transfer Method	Initiated By	Boot	Runtime
XMODEM	Direct Serial VT100	✓	✓
TFTP	Direct Serial VT100	✓	✓
	Ethernet Telnet VT100	✓	✓
	SLIP Telnet VT100	✓	✓
	Ethernet SNMP/IP		✓
	Ethernet SNMP/IPX		✓
	Serial SNMP/SLIP		✓
	Ethernet BOOTP	✓	✓

NOTE: Should the Boot code be corrupted, the hub also supports an XMODEM download from the Preboot XMODEM interface. See the sub-section, "Problems During Downloads" for information about downloading firmware from Preboot.

Different file transfer methods take different amounts of time to execute. This may be important when you choose a transfer method.

Comparison of Download Times

	Method	Time
TFTP	Boot/Runtime download via Ethernet IP or serial port SLIP	40 seconds
XMODEM	Transfer the Flash Boot/Runtime image files via the serial COM port over SLIP	8 minutes at 19.2K baud

All firmware downloads occur from the Boot operating mode. If you start a download while in Runtime mode, the 2824 hub returns to the Boot mode before downloading the firmware. In this case, the STATUS LED turns yellow to indicate the 2824 hub has returned to the Boot operating mode. No SNMP management is available during a firmware download.

The firmware downloaded to the 2824 hub contains both Boot and Runtime binary files. When you start the download, you must choose either Runtime-only or both Boot and Runtime downloads. You can indicate the download through either the VT100 interface or the *n2feTFTPProgramsStatus* MIB variable in the MIB (accessed via SNMP or Compaq Netelligent Management Software).

Download Problems

If an error occurs during the Boot/Runtime download process, the 2824 hub aborts the download. Possible errors include firmware version string error, hardware error (such as the inability to erase or program the Flash), or such non-recoverable errors as excessive TFTP time-outs and bad Flash checksum. The 2824 hub resets and all the LEDs flash to indicate a problem has occurred. If the error did not occur during the erase/program of Boot, you can repeat the download using either the VT100 interface or BOOTP/TFTP (TFTP downloads cannot be initiated using MIB variables since SNMP is not available in Boot).

If Boot code is corrupted due to an unsuccessful download of the Boot firmware, the Preboot firmware lets you download new Boot/Runtime code. In such cases, you must repeat the download using the Preboot XMODEM interface. You can access the Preboot operating mode through the serial COM port of the unit. Then download new firmware using an XMODEM file transfer with a null modem cable or using a remote modem connection via Telnet.

IMPORTANT: The Preboot operating mode does not have in-band communication nor a VT100 interface for initiating downloads. If you need to load the Boot firmware while in Preboot, you must download it from a direct connection to the serial port.

NOTE: The Preboot firmware for 2824 hub is not field-upgradable.

Parameters Stored in NVRAM

The 2824 hub stores important configuration parameters in non-volatile memory to allow its configuration to be saved if a power outage occurs. When the hub is powered up, it restores the saved settings.

- System name, location, and contact
- Novell Hub MIB repeater and port names
- RMON configuration (doesn't include history buckets or event log)
- VT100 configuration, including password
- Port enable/disable
- Backplane isolated/connected
- Backup port configuration
- Port Intrusion configuration, including security
- Internal 2-port 10/100 switch configuration
- IP and SLIP configuration
- IP autodiscovery configuration
- IPX configuration
- IPX autodiscovery configuration
- BOOTP configuration
- IP and IPX trap receivers
- Authentication trap enable/disable
- RFC1516/Novell repeater MIB traps selection
- RMON table configuration timeout
- Modem configuration
- SNMP/IP access control, including community strings
- SNMP/IPX access control, including community strings
- Telnet enable/disable

Compaq Specific Parameters

The following parameters are specific to the Compaq Netelligent 2824 hub.

- **Ethernet Node Address Range** — The 2824 hub must have six unique node (MAC) addresses, each of which consists of six bytes. The first three bytes are fixed and stand for “Compaq Computer Corporation.” The last three bytes must be unique for each interface on the hub.

The following is an example of a MAC address:

00 80 5F VV VV VV

where VV is a byte.

- **Compaq Enterprise Number** — The Compaq private enterprise number is **232**.
- **SysObjectID** — The system object ID contains the following value:

1.3.6.1.4.1.232.101.3.1

- **ifDescr** — The interface description strings contain the following lines:

Agent's Ethernet NIC Interface

Agent's Serial Interface

Common 100Mbps Ethernet collision domain

Unit 1, 100Mbps Ethernet repeater

Unit 1, 10Mbps Ethernet repeater

Unit 2, 100Mbps Ethernet repeater

Unit 2, 10Mbps Ethernet repeater

Unit 3, 100Mbps Ethernet repeater

Unit 3, 10Mbps Ethernet repeater

Unit 4, 100Mbps Ethernet repeater

Unit 4, 10Mbps Ethernet repeater

Unit 5, 100Mbps Ethernet repeater

Unit 5, 10Mbps Ethernet repeater

- **sysDescr** — The system description string contains the following line:
Compaq Netelligent 2000 Fast Ethernet Repeater
- **SAP ID** — This is a Compaq SAP ID registered with Novell. Its hexadecimal value is **b105**. This advertises the Netelligent 2824 service.

Appendix A

Specifications

The following specifications list the physical, electrical, and environmental characteristics of the 2724/2824 Dual-Speed Hub.

Physical

- Unit Weight: 8 lb (4.7 kg)
- Shipping Weight: 13.7 lb (6.2 kg)
- Unit Dimensions: 2.5 x 17 x 13.5 (HxWxD)
- Rubber Foot: 0.25 inches, 0.635 cm high

Electrical

- Power Supply: 90W redundant, hot-swappable
- Cooling: Two 40mm, 12 VDC fans (rear-mounted)
- Power Requirements: Voltage: 100 to 240 VAC
- Frequency: 50 to 60 Hz
- Wattage Consumption: 129W/BTU/hr = 440

Environmental

- Temperature: Operating: 32° to 104° F, 0° to 40° C
Storage: 32° to 140° F, 0° to 60° C
- Humidity: Operating/Storage: 5% to 95% (non-condensing)
- Altitude: Operating: 0 to 10,000 ft, 0 to 3 km
Storage: 0 to 30,000 ft, 0 to 9 km

Appendix B

Using the VT100 Interface

After you set the IP address for the hub, you can use the hub's VT100 interface to view statistics, set specific configuration parameters, and download firmware. The interface's quick access to menu option screens makes it an excellent way to manage the hub if you are unfamiliar with graphical user interfaces (GUIs) or your workstation does not have Compaq Netelligent Management Software installed.

Connecting the Hub for VT100

To access the VT100 interface, connect the hub to a workstation using any one of the following communication methods:

- Direct serial port connection using a modem or a null modem cable (See Chapter 3 – “Installing the Hub” for information about connecting to the serial port.)
- Telnet over IP via an Ethernet connection
- Telnet over SLIP via the serial port connection using a modem or a null modem cable as listed above

Setting Up the Communications Program

You can use a terminal emulator (such as Windows HyperTerminal) or a standard Telnet application to view the VT100 screens. If you use a terminal emulator, set the port settings as follows:

- 9600 bits per second
- 8 data bits
- No parity
- 1 stop bit
- No flow control

Starting the VT100 Interface

After you make the required connections and set up the communications program, follow these steps to start the VT100 interface.

NOTE: The VT100 interface allows only one active user at a time. For example, if an active VT100 session is using Telnet over Ethernet, another session cannot occur over the serial or Ethernet connections.

1. Start the communications program. If you use a Telnet application, enter a valid IP address and start the connection.

2. Enter the following command:

```
vt100
```

NOTE: If the login fails, you may need to retry the connection several times.

The Login screen appears.

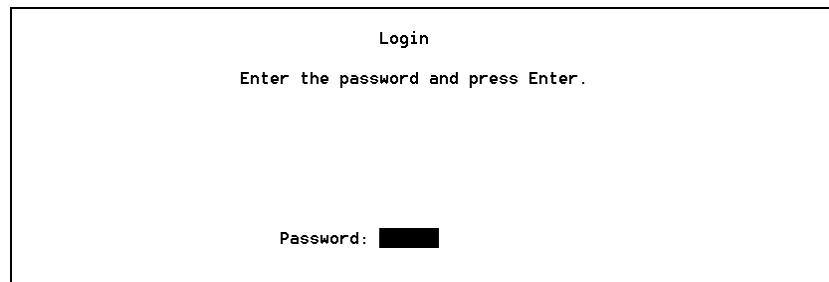


Figure B- 1. Login Screen

3. Within 20 seconds after the Login screen appears, enter the password. The default password is `public`. The Main menu screen appears.
-


```

Main Menu                               IP: 010.001.002.199

Select an option using the cursor keys and Enter, or enter the key letter.

Selection  A

A  System Information
B  Management Agent Configuration
C  Port Statistics
D  Stack Configuration
E  Backup Port Configuration
F  Change UT100 Password
G  Download Firmware
H  Serial Port Setup
I  User Access Configuration
J  Logout

P[2.00]:B[2.00]:R[2.00]                4 hours, 10 minutes

```

Figure B- 2. Main Menu Screen

The main screen displays the Preboot, Boot, and Runtime firmware versions in the lower left corner of the screen. The version identifiers are “P” for Preboot, “B” for Boot, and “R” for Runtime. The value inside the brackets is the version number.

Error Messages

If you enter an incorrect password, the following error message appears:

```
ERROR: Password incorrect, please re-enter
```

You can change the VT100 password by selecting the Change VT100 Password option (F). See “Changing the VT100 Password.”

The default password for VT100 sessions is “public.” If you forget the password, you can restore it to the default password by setting the *cpqnUnitReset* MIB object in the Netelligent Unified MIB to *reset-to-factory-values*(4).



CAUTION: Resetting the password to the default also resets all other durable configuration parameters to their factory settings.

Basic Update Fields

All screens except the Login Screen have three standard update fields that are periodically updated.

- n **System Name** — This field, located at the upper-left corner of each screen, indicates the system name. You can change this name by entering a new name in the System Name field on the System Information Screen or by changing the RFC1213 *sysName* MIB variable. Only the first 25 characters of the name are displayed.
- n **IP Address** — This field, located at the upper-right corner of each screen, indicates the system's IP address. You can change the IP address by entering a new address in the IP Address field on the Management Agent Configuration Screen or by changing the *cpqnIpAddr* MIB variable in the Compaq Unified MIB.
- n **System-Up Time** — This field, located at the lower-right corner of each screen, indicates how long the system has been operating. If the system is up less than one day, this field shows the time in hours and minutes. If the system has been up for more than a day, the field shows the time in days and hours. You cannot change this field unless you reset the hub.

NOTE: The Login Screen displays only the System Name update field.

VT100 Management Options

From the Main menu, you can display data screens that let you perform the following management operations:

- View and edit system information
- Configure the management agent
- View port statistics
- View and edit the stack configuration
- View and edit the backup port configuration
- Change the VT100 password
- Download firmware
- Set up the serial port
- Setting up user access for IP and IPX

Displaying a Data Screen

To select a data screen from the menu, enter the letter that corresponds to the option, or use the arrow keys to highlight the option. Then press <Enter>.

The following table shows the available VT100 screens in the Boot and Runtime operational modes for direct serial port and Telnet connections. Runtime is the normal mode of operation. The Boot screens appear only when the hub executes the Boot sequence or if Runtime is unable to start.

Screen	Boot	Runtime
Login Screen	✓	✓
Boot Main Selection Menu	✓	
Runtime Main Selection Menu		✓
System Information	✓	✓
Management Agent Configuration	✓	✓
Port Statistics		✓
Stack Configuration		✓
Backup Port Configuration		✓
Change VT100 Password	✓	✓
Download Firmware	✓	✓
Serial Port Setup	✓	✓
User Access Configuration		✓
IP User Access		✓
IPX User Access		✓
Logout	✓	✓

Table B-1. Available VT100 Screens in Boot and Runtime

Navigating the VT100 Screens

The VT100 data screens consist of editable and non-editable data fields. Most data screens also display the system up time, system name (first 25 characters), and hub IP address. (The IP address appears only if the hub is connected via a Telnet session.)

Editable fields are highlighted in black. They include *data entry* fields, which require you to enter text, and *toggle* fields, which require you to select a setting from a preset list of options. Toggle fields are enclosed in arrow brackets (< and >).

To edit a data entry field, highlight the field and enter the desired text. To edit a toggle field, highlight the field and press the space bar to toggle through the available options. The new value is active as soon as you change the field.

Each data screen displays unique information and may require keystrokes that differ slightly from other screens. In general, however, use the following keys as described to navigate the data screens.

<Tab> - Press <Tab> to move from field to field in the forward direction. If the field has changed, the new value is recorded when you move to another field. If the value is not valid, an error appears on the screen and the field remains highlighted. You cannot use the <Tab> key to exit a screen.

<Enter> - Press <Enter> to validate an entry or execute an exit option (Cancel changes, Accept changes, or Return to menu). If the entry is not valid, an error appears on screen and the field remains highlighted.

Arrow Keys – Press the right or down arrow keys to move from field to field in the forward direction, or press the left or up arrow keys to move from field to field in a backward direction. If the value of a field has changed, you must press the <Enter> or <Tab> key to record the entry. If you enter invalid information in the field, you can press the arrow keys to restore the previous entry.

<Backspace> - Press <Backspace> to delete a character to the left of the cursor position.

Space Bar – Press the space bar to toggle between options when a toggle field is highlighted. Arrow brackets (< and >) indicate a toggle field.

Arrow Bracket (</>) and Plus/Minus (+ / -) Keys - Some screens use these keys to scroll through information screens for a specific group, interface, or port. For example, the Management Agent Configuration screen uses the arrow bracket keys to scroll through management agent groups. Look at the top of the selected screen to see how these keys function.

Viewing System Information

The System Information screen shows basic information about the system in which the hub operates.

```
System Information                               IP: 010.001.002.199

Contact name Compaq Computer Corporation, 1-800-652-6672
Location
Name

Screen update time    5                      (1..255 Sec.)

Telnet Access        <Enabled >

Reset Unit           <No Reset >

Cancel changes █    Accept changes █                4 hours, 11 minutes
```

Figure B- 3. System Information Screen

The System Information screen displays the following information:

Contact Name — The name of the personal contact at the system installation (also the MIB-II *sysContact* text string)

Location — The location of the system installation (also the MIB-II *sysLocation* text string)

System Name — The designated name of the system (also the MIB-II *sysName* text string)

Screen Update Time — The update time interval in seconds for VT100 screens. The default value is 5.

Telnet Access — Select Enabled or Disabled to enable or disable Telnet access to the hub.

Reset Unit — Select No Reset to prevent the hub from resetting after you accept changes. Select Reset to reset the hub after you accept changes. Select Restore Defaults and Reset the reset the hub and restore all factory default configuration parameters after you accept changes.

Error and Warning Messages

The following error or warning messages can occur if you enter information incorrectly or you attempt to reset the hub system parameters:

ERROR: The value must be in the range [1..255]

WARNING: The unit will be reset

WARNING: The factory default settings will be restored and the unit will be reset

Viewing the Management Agent Configuration

The Management Agent Configuration screen displays information for the hub's Ethernet interfaces and serial interface. The screen consists of the following update fields:

Interface Type — The currently selected interface type. Possible values are “Ethernet” and “Serial.”

Physical (MAC) Address — The physical address of the current interface. This field is blank for the serial interface.

```
Management Agent Configuration   IP: 010.001.002.199

Use '<' and '>' keys to scroll interfaces.

Interface Type:  Ethernet
Physical Address: 0000:7948:0869

Interface Number:      1

IP Address              010.001.002.199
IP Netmask              255.255.000.000
Gateway                010.001.002.001
IP Frame Type          <Ethernet II          >
IPX Frame Type         <Ethernet 802.2      >
SAP Broadcast          <Disabled          >
BOOTP Broadcast        <Disabled          >
BOOTP in Runtime       <Disabled          >
IP Autodiscovery       <Disabled          >
IP Autodiscovery Interval 55                (55..65535 Sec.)
BOOTP Retries          2                    (1..65535)
BOOTP Timeout         5                    (5..255 Sec.)

Cancel changes █      Accept changes █

Return to menu █                                           4 hours, 12 minutes
```

Figure B- 4. Management Agent Configuration Screen

The Management Agent Configuration screen lets you configure the following information for each management agent group:

- **IP Address** — Enter the IP address of the management agent.
- **IP Netmask** — Enter the IP netmask of the management agent.
- **Gateway** — Enter the IP gateway of the management agent.

- **IP Frame Type** — Options include Ethernet II and Ethernet 802.2 SNAP. For management agents that do not have an Ethernet frame type, such as the serial port, the default frame type setting is Not Supported.
- **IPX Frame Type** — Options include Ethernet II, Ethernet 802.3, Ethernet 802.2, and Ethernet 802.2 SNAP. For management agents that do not have an Ethernet frame type, such as the serial port, the frame type setting is Not Supported.
- **SAP Broadcast** — Select Enabled to enable the hub to generate IPX SAP broadcasts every 60 seconds. Select Disable to disable the generation of SAP broadcasts. SAP broadcasts are always disabled for the serial port.
- **BOOTP Broadcast** — Options include Disabled, Enabled-Ethernet II, Enabled-802.2 SNAP, or Enabled-both. BOOTP broadcasts are always disabled for the serial port.
- **BOOTP in Runtime** — Select Enabled or Disabled to enable or disable the BOOTP broadcast configuration in system Runtime operation. For serial interfaces, this field shows “Disabled” and cannot be changed.
- **IP Autodiscovery** — Select Enabled to allow the hub to send out pings for AutoDiscovery. Select Disabled to prevent autodiscovery.
- **IP Autodiscovery Interval** — This field shows the length of time between pings for autodiscovery. Select a value from 55 to 65535 seconds. The default value is 55.
- **BOOTP Retries** — This field shows the number of BOOTP retries the hub will perform on the interface when the hub goes through its Boot sequence (unit is reset or power cycled). Select a value from 1 to 65535. The default value is 2.
- **BOOTP Timeout** — This field shows the amount of time (in seconds) after which a BOOTP attempt times out and the hub can issue another similar request on the interface. Enter a value from 5 to 255 seconds. The default value is 5.

Error Messages

The following error messages can occur if you enter information incorrectly:

ERROR: The field value must be in the range [0...255]

Viewing Port Statistics

The Port Statistics screen displays statistics for specific ports on the hub.

PORT STATISTICS		IP: 010.001.002.199			
Use '<' and '>' keys to scroll ports. Use '+' and '-' keys to scroll units.					
	Port 1	Port 2	Port 3	Port 4	
Readable Frames	0	83	0	7,896	
Readable Octets	0	67,329	0	669,154	
Collisions	0	0	0	1	
FCS Errors	0	0	0	0	
Alignment Errors	0	0	0	0	
Frames Too Long	0	0	0	0	
Short Events	0	0	0	0	
Very Long Events	0	0	0	0	
Data Rate Mismatch	0	0	0	0	
Autopartitions	0	0	0	0	
Last Src Address	0000:0000:0000	0000:79C4:001A	0000:0000:0000	0000:79A8:004C	
Src Address Chgs	0	1	0	1	
Port Speed	No Link	Auto:10Mbps	No Link	Auto:100Mbps	
Port Link	Down	Up	Down	Up	
Port State	< Enabled >	< Enabled >	< Enabled >	< Enabled >	
Return to menu	Scroll	Unit 1	4 hours, 13 minutes		

Figure B- 5. Port Statistics Screen

In addition to port statistics, the Port Statistics screen displays the following information:

- n **Port Speed** — Shows the current wire speed of the port which includes the following options:
 - o No Link — No connection on this port
 - o Auto: 100Mbps — The port has auto-negotiated to 100Mbps
 - o Auto: 10Mbps — The port has auto-negotiated to 10Mbps
 - o Fixed: 100Mbps — The port is a 100Mbps-only port, such as a SUM port or a Netelligent 2524/2624 RJ-45 port, or the port is administratively forced to 100Mbps
 - o Fixed: 10Mbps — The port is forced, either administratively or via a front-panel switch, to operate at 10Mbps
- n **Port Link** — This field has three possible settings: Partition (port is auto-partitioned), Up (link is present), and Down (link is not present).

Port State — Select Enabled or Disabled to enable or disable a port. The changed setting takes effect immediately.

To scroll forward or backward to other ports, move the cursor to the Scroll field and press the < and > keys. To scroll forward or backward to other units, move the cursor to the Scroll field and press the - and + keys.

Shortcut: You can change the Scroll setting to scroll up to nine ports at a time (the default is one, as shown in Figure B-5). When you press the < and > keys, the screen scrolls the specified number of ports.

NOTE: Refer to the glossary for definitions of these statistics.

Viewing the Stack Configuration

The Stack Configuration screen displays configuration information for all hubs in a stack. If a hub is powered down or not present in the stack, dashes appear in that hub's row. The screen displays information for three units if the managing hub is a 2624 and five units if the managing hub is a 2824.

Stack Configuration		IP: 010.001.002.199	
Unit Number	Unit Description	Backplane Configuration	Internal 10/100 Switch Configuration
1	CPQN2824	<Connected>	<Enabled>
2	CPQN2524	<Connected>	<N/A>
3	-----	<----->	<----->
4	-----	<----->	<----->
5	-----	<----->	<----->

Return to menu ■ 4 hours, 13 minutes

Figure B- 6. Stack Configuration Screen

Unit Number — The screen shows the unit numbers in ascending order, with unit description, backplane status, and internal 10/100 switch status.

Unit Description — This field shows a brief description of the hub.

Backplane Configuration — The backplane connection status for the hub. Select “Connected” or “Isolated” to connect the hub to or isolate it from the stack’s common 100Mb/s Ethernet backplane. For Netelligent 2524 and 2624 hubs, which do not have this feature, this field always shows “Connected.”

Internal 10/100 Switch Configuration — Select “Disabled” to disable the internal switch and isolate the 10Mb/s and 100Mb/s collision domains. Select “Enabled” to enable the internal switch.

NOTE: If the selected hub is a 2724 (manageable) unit and its internal 10/100 switch has been disabled via the hub’s hardware DIP switch, you cannot enable the switch using this field. For 2524 and 2624 hubs, this field always shows “N/A.”

Error Messages

The following error messages can occur while modifying the stack configuration:

ERROR: This unit cannot be isolated from the backplane.

ERROR: Cannot enable/disable internal switch on this unit

Viewing and Editing the Backup Port Configuration

The Backup Port Configuration screen shows information about the slot number of the primary and backup port and the status of the ports. The screen also lets you add, delete, and enable or disable the state of backup port entries.

```

Backup Port Configuration      IP: 010.001.002.199

Use '+'/ '-' keys in the 'Action' field to select an entry.

Entry   Primary   Primary   Backup   Backup   State
        Unit     Port     Unit     Port
-----
--      --      --      --      --      --
--      --      --      --      --      --
--      --      --      --      --      --
--      --      --      --      --      --
--      --      --      --      --      --
--      --      --      --      --      --
--      --      --      --      --      --
--      --      --      --      --      --
--      --      --      --      --      --
--      --      --      --      --      --
--      --      --      --      --      --
-----
--      --      --      --      --      --> Action
--      --      --      --      --      --> None

Return to menu █                               4 hours, 14 minutes
  
```

Figure B- 7. Backup Port Configuration Screen

Adding a Backup Port Entry

To add a backup port entry, follow these steps:

1. From the Action field, move the cursor to the Primary Unit entry field. Then enter the number of the desired primary unit.
2. Move the cursor to the Primary Port entry field. Then enter the number of the desired primary port.

.....
B-16 *Using the VT100 Interface*

3. Move the cursor to the Backup Unit entry field. Then enter the number of the desired backup unit.
4. Move the cursor to the Backup Port entry field. Then enter the number of the desired backup port.
5. Move the cursor to the State entry field and press the space bar to select Enable or Disable.
6. Move the cursor to the Action field and press the space bar until Add appears.
7. Press the **Enter** key. The new backup port entry appears in the backup port configuration list.

Deleting a Backup Port Entry

To delete a backup port entry, follow these steps:

1. When the cursor at the Action field, press the - or + keys to highlight a backup port entry.
2. Move the cursor to the Action field and press the space bar until Delete appears.
3. Press the **Enter** key.

When you delete an entry, the backup port remains disabled. To enable the port, see the section “Port Statistics” in this chapter.

Updating the State of a Backup Port Entry

To update the state of a backup port entry, follow these steps:

1. Position the cursor in the Action field.
 2. Press the - or + keys to highlight a backup port entry.
 3. Move the cursor to the State entry field.
 4. Press the space bar until the desired option (Disabled or Enabled) appears.
-

5. Press the **Enter** key.

Error Messages

The following error messages may appear if you enter information incorrectly in the Backup Port Configuration window:

“ERROR: Unable to set backup port”

“ERROR: Unable to set backup status”

“ERROR: Unable to delete”

“ERROR: Unable to update status”

To correct the error, be sure you have correctly entered all the necessary information in the various fields, including valid port and backup port numbers.

Changing the Password

The Change Password screen lets you change your current password. To change your password, follow these steps:

1. Enter the old password in the Old password field.

NOTE: You must enter information in the Old password field to advance the cursor to the New and Verify password fields.

2. Enter the new password in the New password and Verify password fields and press the **Enter** key.

```
Change UT100 Password          IP: 010.001.002.199
Type old and new passwords, then re-type new password and press Enter.

Old password: ██████████
New password: ██████████
Re-type new password: ██████████

Cancel changes █              4 hours, 14 minutes
```

Figure B- 8. Change VT100 Password Screen

The default password for VT100 sessions is “public.” If you forget the password, you can restore it to the default password by setting the *cpqnUnitReset* MIB object in the Netelligent Unified MIB to *reset-to-factory-values(4)*.



CAUTION: Resetting the password to the default also resets all other durable configuration parameters to their factory settings.

Error Messages

The following error messages can occur if you have incorrectly entered information in the Change Password window:

ERROR: Old password not valid, please re-enter

ERROR: Re-typed password does not match new password

Downloading Firmware

The Download Firmware screen lets you download an updated version of firmware. You can download Runtime only or a combination of Boot and Runtime. If you access VT100 using a direct link, you can download firmware via XMODEM or TFTP over Ethernet. If you access VT100 using Telnet, you can download firmware via TFTP over Ethernet or TFTP over SLIP. Null modem SLIP connections can only occur at 9600 baud. SLIP connections over a remotely linked modem are available at 2400, 9600, and 19.2K baud.

```
Download Firmware                               IP: 010.001.002.199
Toggle selections to download firmware.

Download type  <Runtime only>
Protocol type  < XMODEM >
Version       ██████████

TFTP Firmware Download Parameters
(required only for a TFTP download)

TFTP server IP address 000.000.000.000
Filename ████████████████████████████████████████████████████████████████████████████

Return to menu █ Start download █                               4 hours, 15 minutes
```

Figure B- 9. Download Firmware Screen

To download firmware, follow these steps:

1. Position the cursor on the Download Type field. Press the space bar to select Runtime Only or Boot/Runtime.
2. Position the cursor on the Protocol type field. Press the space bar to select the desired option (XMODEM, TFTP, and so forth).
3. Position the cursor on the Version field and enter the firmware version, including any leading zeros (no periods). This information must be correct for a successful download. You can find the version string in the release notes that come with the firmware.

.....
B-20 *Using the VT100 Interface*

4. If you selected TFTP as the protocol type, enter the TFTP server IP address in the TFTP server IP address field and enter the firmware image filename in the Filename field.
5. To execute the download, position the cursor on the Start download field and press <Enter>. Or, to cancel the download and return to the Main menu screen, position the cursor on the Return to menu field and press the **Enter** key.

Error Messages

The following error messages may appear if you enter information incorrectly in the Download Firmware window:

ERROR: The field must be in the range [0..255]

ERROR: Invalid parameter set

ERROR: Version string invalid

ERROR: Invalid product identifier

ERROR: Invalid version identifier

ERROR: Invalid unit type

ERROR: Invalid major version number

To correct the error, be sure you have entered the correct parameters and version string. Be sure the spelling and number sequences are correct. If the error message continues to appear, contact Compaq Technical Support.

Setting Up the Serial Port

The Serial Port Setup screen lets you set up the hub's serial port configuration parameters.

The Current Baud Rate field shows the baud rate that the serial port is currently operating on.

```

Serial Port Setup                               IP: 010.001.002.199

Enter the parameters for configuration of serial ports.

Port Number                                     1
Current Baud Rate                               9600

Auto Baud Selection   <Disabled>
Baud Rate             <9600 >
Send Init String      <Enabled >
Initialization String AT&FX1E000U1&C1S0=1S12=5
Auto Negotiation      <Disabled>

Cancel changes █      Accept changes █

Return to menu █                                           4 hours, 15 minutes
  
```

Figure B- 10. Serial Port Setup Screen

The Serial Port Setup screen lets you modify the following information:

Port Number — This field applies only to multi-serial port systems.

Auto Baud Selection — Select “Enabled” and “Disabled” to enable or disable the function of automatically cycling through the supported baud rates to look for modem connection. The default setting is “Disabled.”

Baud Rate — Select from the available baud rates of “2400,” “9600,” or “19200” if auto baud selection is disabled. If auto baud is enabled, this field displays “Auto.”

Send Init String — Select “Enabled” or “Disabled” to enable or disable the hub’s ability to allow the serial port to send out the modem initialization string. The default setting is “Enabled.”

Initialization string — This information is the text string to initialize the modem. Although you can customize this string, the recommended modem initialization string is AT&FX1E0Q0V1&C1S0=1S12=5: factory setting, smartmodem 1200 mode, echo off, modem response on, verbose on, DCD asserted during carrier linkage, auto-answer on 1 ring, escape sequence guard time = 100mS. If you choose to enter a new modem command string, the string can be up to 40 characters in length. However, in order for the hub to work correctly, the following modem parameters must remain set to their default values: modem response on, verbose on, DCD asserted during carrier linkage, auto-answer on, and echo off.

Auto negotiation — Always “Disabled”

Configuring User Access

The user access screens let you configure user access for IP and IPX. This feature allows the management agent to limit SNMP and Telnet access to authorized stations. (You Enable/Disable Telnet through the System Information screen.)

When you select the User Access Configuration option, the following menu appears. From this menu, select the desired address type (IP or IPX).

```

User Access Menu                               IP: 010.001.002.199
Select an option using the cursor keys and Enter, or enter the key letter.

Selection A
A IP User Access Configuration
B IPX User Access Configuration
C Return to Main Menu

4 hours, 16 minutes
```

Figure B- 11. User Access Menu

Configuring IP User Access

The IP User Access Configuration screen lets you configure IP user access parameters. Each entry specifies an IP address range via an address mask, address match, write community string, and access description.

```
IP User Access Configuration IP: 010.001.002.199
Use the '+' and '-' keys in the 'Action' field to select an entry.
-----
  Address Mask      Address Match      Community          Access
-----
  000.000.000.000  000.000.000.000  public            RW Telnet
-----
  -----
  -----
  -----
  -----
  -----
-----
  ---.---.---.---  ---.---.---.---  public           < No Access >
                                     Action < None >
Return to menu █                                     4 hours, 17 minutes
```

Figure B- 12. IP User Access Configuration

The hub's management agent lets you specify a range of authorized addresses or a list of individual nodes. The agent treats the requestor's address, address mask, and the address match as a string of bits. The following examples describe two ways to set up user access for IP.

Example 1

Suppose a user wanted all nodes on a specific IP or IPX segment to have SNMP access. In this case, the address mask should have 1s in the network part of the IP/IPX address and 0s in the node part of the address. The address match should have the network number in the network part of the IP/IPX address and 0s in the node part of the address.

Mask	Match	Result
255.255.255.0	143.162.103.0	All nodes on IP network 143.162.103 pass
FFFFFFFF:000000000000	01ABCDEF:000000000000	All nodes on IPX network 01ABCDEF pass

Example 2

Suppose a user wanted a specific node on a specific IP or IPX segment to have SNMP access. In this case, the address mask should have 1s in both the network part of the IP/IPX address and the node part of the address. The address match should have the network number in the network part of the IP/IPX address and the node address in the node part of the address.

Mask	Match	Result
255.255.255.255	143.162.103.73	Only IP address 143.162.103.73 passes
FFFFFFFF:FFFFFFFFFFFF	01ABCDEF:00805F39AE62	Only IPX address 01ABCDEF:00805F39AE62 passes

If an SNMP request passes the address mask/match check, the agent compares the requestor's community string with the authorized community string. If that check passes, the agent compares the SNMP request with the node's authorized rights (see the Netelligent Unified MIB for a description of rights). If all checks pass, the agent processes the SNMP request. Otherwise, the agent discards the request and issues an authentication failure trap.

Access Options

The Access field at the end of the edit line lets you select the following access options:

No Access — The address/community name pair has neither SNMP/IP nor Telnet access.

RO/No Telnet — Allows only read access to MIB objects and disallows Telnet access.

RO/Telnet — Allows only read access but the station can initiate a Telnet session.

RW/Telnet — Allows full access to the device's MIB and allows the station to initiate a Telnet session.

NOTE: Telnet access is either allowed or disallowed. Generally, devices do not have read-only Telnet sessions.

Adding an Entry

Follow these steps to add an entry.

1. Move the cursor to the Action field, toggle to the Add option (using the space bar), and press <Enter>.
2. Enter the information for the new entry in the edit line.
3. Move the cursor to the Action field, toggle to the Update option, and press <Enter>.

Modifying an Entry

You can configure up to eight entries for IP access. To modify an entry, follow these steps:

1. Select an entry by placing the cursor in the Action field and pressing the “+” and “-“ keys to highlight the entry. The currently selected entry appears in the edit line above the Action field for modification.
-

2. Move the cursor to the edit line and modify the three edit fields as desired.
3. Move the cursor to the Action field, toggle to the Update option (using the space bar), and press <Enter>. The new configuration immediately takes effect. If there are any configuration errors, an error message appears.

You can configure up to eight entries without exiting the screen. Repeat Steps 1-3 to modify additional entries.

Deleting an Entry

Follow these steps to delete an entry.

1. Select an entry by placing the cursor in the Action field and pressing the “+” and “-“ keys to highlight the entry. The currently selected entry appears in the edit line above the Action field.
2. Move the cursor to the Action field, toggle to the Delete option, and press <Enter>. The entry disappears from the table.

Error Messages

The following error messages could appear as you enter information on the IP User Access Configuration screen.

ERROR: The field must be in the range [0..255]

ERROR: Invalid address mask and address match pair

Configuring IPX User Access

The IPX User Access Configuration screen lets you configure IPX user access parameters. Each entry specifies an IPX address range via an address mask, address match, write community string, and access description.

```

IPX User Access Configuration IP: 010.001.002.199

Use the '+' and '-' keys in the 'Action' field to select an entry.

  Address Mask      Address Match      Community      Access
-----
00000000:000000000000 00000000:000000000000 public          RW
-----
-----
-----

-----:-----:----- public <No Access>
                                     Action <None>

Return to menu █                                     4 hours, 16 minutes
  
```

Figure B- 13. IPX User Access Configuration

The hub's management agent lets you specify a range of authorized addresses or a list of individual nodes. The agent treats the requestor's address, address mask, and the address match as a string of bits. For examples of setting IPX user access, see Examples 1 and 2 under "Configuring IP User Access."

Access Options

The Access field at the end of the edit line lets you select the following access options:

No Access — The address/community name pair has no SNMP/IPX access.

RO — Allows only read access to MIB objects.

RW — Allows full access to the device's MIB.

Adding an Entry

Follow these steps to add an entry.

1. Move the cursor to the Action field, toggle to the Add option (using the space bar), and press <Enter>.
2. Enter the information for the new entry in the edit line.
3. Move the cursor to the Action field, toggle to the Update option, and press <Enter>.

Modifying an Entry

You can configure up to four entries for IPX access. To modify an entry, follow these steps:

1. Select an entry by placing the cursor in the Action field and pressing the “+” and “-“ keys to highlight the entry. The currently selected entry appears in the edit line above the Action field for modification.
2. Move the cursor to the edit line and modify the three edit fields as desired.
3. Move the cursor to the Action field, toggle to the Update option (using the space bar), and press <Enter>. The new configuration immediately takes effect. If there are any configuration errors, an error message appears.

You can configure up to four entries without exiting the screen. Repeat Steps 1-3 to modify additional entries.

Deleting an Entry

Follow these steps to delete an entry.

1. Select an entry by placing the cursor in the Action field and pressing the “+” and “-“ keys to highlight the entry. The currently selected entry appears in the edit line above the Action field.
2. Move the cursor to the Action field, toggle to the Delete option, and press <Enter>. The entry disappears from the table.

Error Messages

The following error messages could appear as you enter information on the IPX User Access Configuration screen.

ERROR: Invalid address mask and address match pair

Logging Out of the Management Session

The Logout screen lets you end the VT100 management session. If you select Yes, the Login screen reappears and you have 10 seconds to retype the password if desired. Otherwise, the VT100 session ends.

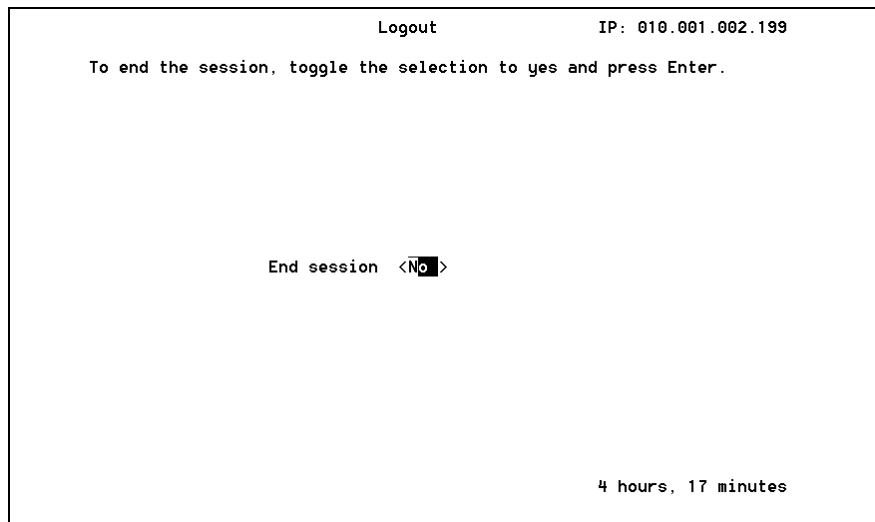


Figure B- 14. Logout Screen

Glossary

100Base-FX	An implementation of the IEEE 802.3 Fast Ethernet standard on multimode fiber cable with SC-type connector with one pair of fiber cable. Stations are connected using a star topology.
100Base-TX	An implementation of the IEEE 802.3 Fast Ethernet standard on Category 5 UTP with two pairs of wires. Stations are connected using a star topology. The maximum segment length is 100 meters.
802.2	An IEEE standard that governs Logical Link Control. The LLC layer can provide either connection oriented services, connectionless services, or a combination of both.
802.3	An IEEE standard that governs Carrier Sense Multiple Access with Collision Detection (CSMA/CD) networks. 802.3, or Ethernet, operates on different cable types (for example, UTP, coaxial, and fiber).
802.3u	A supplement to 802.3 that governs Carrier Sense Multiple Access/Collision Detection (CSMA/CD) for 100Mbps networks. This supplement covers the specifications for 100Base-T4, TX, and FX.
802.3 RAW	802.3 RAW uses the packet format defined by the 802.3 IEEE standard without additional header support such as 802.2.
ARP	<i>See</i> Address Resolution Protocol.
Address Resolution Protocol	Used by the TCP/IP protocol stack to dynamically bind an IP address with a MAC address. This is defined in RFC826.
Autodiscovery	The ability of a network manager to discover the node address and functionality of network devices. The 2824 hub supports IP and IPX autodiscovery.

Flash	A memory device that allows unlimited read and limited write (approximately 100K) cycles.
FCS	<i>See</i> Frame Check Sequence Errors.
Frame Alignment Errors	A frame alignment error occurs when a packet is received but not properly framed (that is, not a multiple of 8 bits).
Frame Check Sequence Errors	Errors that occur when a packet is involved in a collision or is corrupted by noise.
Frames Received OK	The number of frames received without error.
Frames Too Long	Frames that are longer than the maximum length of a proper Ethernet frame, but not as long as frames resulting from jabbering.
FX	100Base-T standard for Fast Ethernet based on fiber. The SUM module provides duplex SC and ST connectors for 100Base-FX.
Hot Swappable	Ability to add or remove a module or power supply without removing power.
ICMP	Internet Control Message Protocol. Provides error handling and control messages for TCP/IP.
IP	Internet Protocol. A protocol that provides connectionless, best-effort datagram delivery service.
IP Address	The Internet Protocol address assigned to a hub, module, or node.
IPX	Internetwork Packet Exchange. A Novell NetWare protocol that provides a connectionless datagram service.
IPX Diagnostics	IPX diagnostics are required to support the Novell NetExplorer server. The NetExplorer server is used to update the Novell ManageWise database with the current network configuration.

G-4 Glossary

Jabbering	Continuous transmission from a node, generally as a result of hardware or firmware failure.
Latency	The time duration from when the first preamble bit of a packet enters one port to when the first preamble bit of that same packet exits another port.
Link Test	A link test is performed by the port hardware before transmit and receive functions are enabled to ensure the integrity of the cable (the link).
MAC	<i>See Media Access Controller.</i>
MAC Address	The Ethernet MAC address is a 6-byte node address. All Ethernet node addresses are unique.
Manageable	A hub is manageable if it does not contain management agent firmware. Manageable units can be managed only if they are attached to a managing unit.
Management Information Base	Describes an agent's configuration flexibility, diagnostic ability and information that can be reported to a network management station.
Managing	A hub is <i>managing</i> if it contains management agent firmware. A Netelligent 2824 managing unit can communicate over Ethernet and over its serial port.
MDI	UTP contact assignments without internal crossover.
MDI-X	UTP contact assignments with internal crossover.
Media Access Controller	A device that governs access to transmission media.
MIB	<i>See Management Information Base.</i>
MII	Media Independent Interface
NIC	Network Interface Controller. Connects a node to a

	network.
NMS, Novell	Novell's NMS (NetWare Management System) is an integrated network management system that provides a platform for managing a multivendor, heterogeneous network environment. NMS can autodiscover network services by monitoring transmitted SAP IDs. NMS is part of ManageWise.
Nonvolatile Random Access Memory	Electronic circuitry that provides back-up operation of CMOS RAM and/or Flash PROM in case of a power failure.
NVRAM	<i>See</i> Nonvolatile Random Access Memory.
Octet	An octet consists of 8 bits (that is, a byte).
Octets received OK	The number of octets (bytes) received without error.
Partition	The electrical disconnecting of a node from a LAN at its point of connection to a hub. The node remains physically attached. A node can be autopartitioned by the hardware based on network errors.
PDU	<i>See</i> Protocol Data Unit.
Port	An external connector in which a cable is plugged and to which PCs and other node devices on the network connect.
POST	Power On Self Test
Protocol Data Unit	A packet that contains control information and optional data.
RIP	Routing Information Protocol (RIP) is the routing protocol used by IPX routers. It optimizes the routing between source and destination addresses by minimizing the "hop" count. The firmware supports RIP to allow NMS to ascertain the 2724/2824 hub's MAC address, thus allowing NMS to initiate SNMP over IPX communications.

Serial Line IP	A protocol that provides a method of transporting IP datagrams over a serial connection.
Service Advertising Protocol	A protocol that sends service information to all nodes on an IPX network.
Simple Network Management Protocol	A protocol used by network management stations to communicate management information over a UDP/IP or IPX network.
SLIP	<i>See</i> Serial Line IP.
SNMP	<i>See</i> Simple Network Management Protocol.
T4	100Base-T standard for Fast Ethernet based on 4 wire pairs using Category 3, 4, or 5 cable.
TFTP	<i>See</i> Trivial File Transfer Protocol.
Trap	A trap is an unsolicited SNMP event sent from an agent to a network management station. Traps can include cold start, port autopartition and backup port enabled.
Trivial File Transfer Protocol	A protocol that can be used to download a new Flash image.
TX	100 Base-T standard for Fast Ethernet based on 2 wire pairs using Category 5 cable.
UART	<i>See</i> Universal Asynchronous Receiver.
UDP	<i>See</i> User Datagram Protocol.
Universal Asynchronous Receiver	Provides hardware support for serial communications.
Unshielded Twisted Pair	A type of network cable that is usually connected using RJ-45 connectors.
User Datagram	A protocol that provides unreliable connectionless delivery

.....

G-8 *Glossary*

Protocol	service using IP. It adds the ability to distinguish among multiple destinations within a given host.
UTP	<i>See</i> Unshielded Twisted Pair.
XMODEM Protocol	XMODEM is a serial communications protocol used to transfer ASCII or binary data. XMODEM uses 8-bit characters and transfers data using 128-byte blocks, each of which is followed by a checksum or CRC. If the checksum (CRC) on a block is correct, the next block is sent; otherwise the same block is retransmitted.

Index

1

10 COL LED 1-7
 10 Mb/s - 100 Mb/s switch 1-3
 10 MBPS LED 1-8
 10 MDI - 10/100 MDI-X switch 1-11
 10 ONLY - 10/100 switch 1-10, 1-11
 10/100 SW LED 1-8
 100 BP LED 1-8
 100 COL LED 1-7
 100Base-FX 2-4, 3-5
 100Base-TX 2-3
 100MBPS LED 1-8
 10Base-T 1-1

A

Activity LED 1-8
 Adding hubs to stack 3-6
 Address Resolution Protocol 5-6
 Alarm group 5-15
 Alarm table 5-15, 5-16
 AlarmStartupAlarm 5-16
 ALT LED 1-8
 Altitude 2-1
 Autodiscovery 1-3

B

Backplane connection 1-10
 Backplane connection cable 3-6, 3-8
 Backup ports 1-2
 Bindery entries 5-10
 Bits per second 4-3
 Boot 4-7
 Boot code 5-18
 BOOTP 5-6
 request 4-7, 5-2
 response 5-5
 retries 5-2

 retry interval 5-2
 server 4-7
 Broadcast filtering 1-3

C

Cable
 connecting 3-5
 length 3-5
 requirements 2-2
 type 2-4
 Cabling chart 2-6
 Class I repeater 1-1, 1-5
 Clearance 2-1
 Collision LED 1-8
 COM1 properties 4-4
 Compaq
 enterprise number 5-20
 Netelligent 2000 Fast Ethernet
 MIB 5-3
 Netelligent Management
 Software 5-8
 SAP ID 5-21
 parameters 5-20
 Component description 1-5
 Configuration parameters 5-2
 Configuring hub for management 4-1
 Connection speed 1-11
 Copper wire 2-3
 CpqnIpAddr MIB 5-5
 CpqnIpFrameType
 MIB object 5-5
 Crossover twisted-pair wiring 2-4
 CSMA/CD 2-3

D

Data bits 4-3
 DB9 connector 1-8, 3-11
 Default gateway 4-7
 Default settings 5-2
 Dimensions 2-2
 DIP switch settings 3-6
 Download problems 5-18

E

- EIA 19-inch rack 3-1
- Electrical requirements 2-1
- Electrical shock 2-2
- Electromagnetic interference 2-3
- Enterprise number 5-20
- EnterpriseSpecific traps 5-11
- Environmental requirements 2-1
- EtherHistoryTable 5-14
- Ethernet
 - BOOTP 5-17
 - frame type 5-3, 5-4
 - frames 5-7
 - history table 5-14
 - IP 5-17
 - IP communications 5-4
 - NIC Interface 5-20
 - node address range 5-20
 - repeater MIB, Novell 5-3
 - SNMP/IP 5-17
 - SNMP/IPX 5-17
 - statistics table 5-13
 - topologies 5-4
- ETHERNET_802.2 5-8
- ETHERNET_II 4-7, 5-5
- ETHERNET_SNAP frame type 5-4, 5-5
- Event group 5-16
- Event table 5-12, 5-15, 5-16
- Expansion interface 3-6
- Expansion ports 3-9

F

- Falling alarm 5-15, 5-16
- Fast Ethernet 2-2, 2-3, 2-4, 3-6, 5-3
- Firmware 5-7, 5-18
 - Boot 5-18
 - Preboot 5-18
 - TFTP 5-6
 - updates 1-2, 5-17

- Flow control 4-3
- Frame types 4-7
- Frequency 2-1
- Front panel 1-5
- Full-duplex operation 3-5

G

- Group change 5-12

H

- Hexadecimal value 5-21
- History control table 5-14
- History group 5-14
- HMI hubs 5-9
- HMI-compliance mechanism 5-10
- Host hub 3-9
- HOST setting 3-7
- HOST/TARGET switch 1-2, 1-9, 3-6
- Hub
 - attaching rubber feet 3-1
 - invalid connections 3-7
 - mounting 3-1
 - positioning in rack 3-2
 - rack mounting 3-1
- Humidity 2-1
- HyperTerminal 4-1

I

- ICMP pings 5-7
 - IEEE 802.3u specification 2-3, 2-4
 - Installation 3-1
 - Installation requirements 2-1
 - Interconnecting hubs 3-6
 - Interface description 5-20
 - Internal switch, disabling 1-10
 - Internet Control Messages Protocol 5-6
 - Intrusion detection 1-2
 - Invalid connections 3-7
-

- IP
 - address 4-1, 4-7, 5-2
 - frame type 5-2
 - gateway 5-2
 - network mask 5-2
 - trap receivers 5-2
- IP autodiscovery
 - enable 5-2
 - ping interval 5-2
- IPX
 - address 5-2, 5-11
 - autodiscovery support 5-10
 - communications 5-8
 - diagnostics 5-9, 5-10
 - frame type 5-2, 5-8
 - network number 5-8, 5-9
 - packets 5-8
 - protocol stacks 5-3
 - routers 5-8
 - traffic 5-8
 - trap receiver addresses 5-8
 - trap receivers 5-2
 - trap tables 5-11
- Isolating segment 1-12
- L**
- LED indicators 1-2, 1-6
 - table 1-7
- Log table 5-16
- Login screen 4-5
- Logout screen 4-7
- M**
- MAC address 4-7, 5-20
- Main menu screen 4-5, 4-6
- MAN setting 3-8, 3-9
- MAN/UNM switch 1-10
- Manageable hub 1-1
- Management
 - agent 1-1
 - features 5-1
 - firmware 1-1
 - methods 5-1
- Management Agent Configuration
 - screen 4-6, 5-5
- Managing hub 1-1
- MDI 1-11
- MDI-X 1-11
- MIB objects 5-7, 5-8, 5-11
- MIBs supported 5-3
- Migration 1-1
- MODE button 1-8
- Modem 3-11, 3-13
- Modification methods 5-2
- Mounting brackets 3-2
- Multicast filtering 1-3
- N**
- Netelligent
 - Management Software 4-1
 - Unified MIB 5-11
- Network parameters 5-1
- Novell 5-7, 5-8, 5-21
 - Ethernet Repeater MIB 5-3
 - IPX autodiscovery 5-10
 - name 5-3
- Null modem 3-11, 3-12
- NVRAM 5-3
 - resources 5-16
 - stored parameters 5-19
- O**
- One-to-one cable pinout 2-3
- Optic cable 2-4
- Overview 1-1
- P**
- Package contents 1-4
- Parity 4-3

- Password 4-5
- Pinout 2-3
- Planning switch installation 2-1
- Polling interval 5-14
- Port settings 4-3
- POST 1-6
- Power
 - connecting 3-10
 - cord 1-4, 3-10
 - disconnecting 3-11
 - LED 1-7, 3-10
 - outlet 2-2
 - requirements 2-1
- Preboot XMODEM interface 5-17, 5-18

R

- Rack inventory chart 2-7
- Rack-mounting 3-1
- RFC1157 generic trap category 5-11
- RFC1213 MIB 5-3
- RFC1516 MIB 5-3
- RFC1516 trap 5-12
- RFC1757 MIB 5-3
- RIP broadcasts 5-8
- Rising alarm 5-15
- RJ-45 port 1-2, 1-5, 3-5
- RMON 1-2, 5-1, 5-13
 - alarmTable 5-12
- Rubber feet 3-1
- Runtime 4-7
 - binary files 5-18

S

- SAP
 - broadcast 5-2, 5-8
 - ID 5-21
- SC-type connector 2-4, 3-3, 3-5
- Segment 1-12
- Segmentation 1-12

- Serial COM port 1-8, 3-11
- Serial interface 5-20
- SLIP 1-8
 - address 5-2
 - gateway 5-2
 - network mask 5-2
- Smart Uplink Module 3-3
 - 50-pin connector 3-4
 - inserting 3-3
 - LEDs 1-6
 - port 1-5, 3-3
 - socket 3-4
- SNMP 1-2, 1-8, 5-1, 5-6
 - management 5-3, 5-10, 5-18
 - management platforms 5-6
 - over IP 5-5
 - over IPX 5-10
 - trap 5-8, 5-15, 5-16
- Spatial requirements 2-2
- Spring screws 3-4
- Stack 3-6
- Stack Configuration screen 1-12
- Stackable 1-2
- Statistics 1-3
- Statistics group 5-13
- STATUS LED 1-7, 3-7, 3-8, 4-7, 5-18
- Stop bits 4-3
- Straight-through twisted-pair wiring 2-4
- ST-type connector 2-4, 3-3
- Subnet mask 4-7
- SW EN/SW DIS switch 1-10, 3-6
- System
 - description 5-21
 - object ID 5-20
 - planning charts 2-5

T

- Target hub 3-9
- TARGET setting 3-7, 3-8

TCP 5-6
Telnet 1-8, 5-3, 5-5, 5-6, 5-10, 5-18
Telnet VT100 5-17
Temperature 2-1
Terminal emulation 4-1
TFTP 5-6, 5-17
 serial COM port operation 1-8
Threshold 5-16
Topologies, Ethernet 5-4
Twisted-pair
 specifications 2-2
 cable 3-5
TX connector 3-3

U

UNM setting 3-7, 3-8
UNM/MAN switch 3-6
Unmanaged stack 3-6
Unshielded twisted pair 2-3
User Datagram Protocol 5-6
UTP 1-3, 1-5, 2-2
 requirements 2-3

V

Variable bindings 5-11
Voltage 2-1
VT100 1-12, 4-1, 5-1
 emulation 5-3
 interface 1-2, 1-8, 4-7, 5-8

W

Wiring guage 2-2

X

XMODEM 1-8, 5-17



COMPAQ

©1997 Compaq Computer Corporation. All rights reserved.
Compaq Registered U.S. Patent and Trademark Office.
Company and product names mentioned herein may be
trademarks and/or registered copyright and trademarks of
their respective companies.